Abordări strategice privind riscurile de securitate legate de implementarea tehnologiei 5G și de utilizarea sistemelor de recunoaștere facială

Florina VEVERA
IF Idea Factory Think Thank
florinasvevera@gmail.com

Rezumat: Articolul își propune o trecere în revistă a măsurilor întreprinse la nivel european pentru mitigarea riscurilor de securitate legate de implementarea rețelelor 5G în spațiul comunitar, dar și argumentele generate de SUA și măsurile întreprinse cu privire la subiectul Huawei. Totodată sunt avute în vedere și oportunitatea, viziunea și măsurile întreprinse pentru stabilirea unui cadru legislativ și etic pentru utilizarea tehnologiilor de recunoaștere facială care să protejeze confidențialitatea datelor cu caracter personal, dar și viața privată a cetățenilor.

Cuvinte cheie: rețele 5G, sisteme de recunoaștere facială, GDPR, securitate cibernetică.

Strategic approaches concerning the security risks related to the implementation of the 5G technology and the use of facial recognition systems

Abstract: This article aims to review the measures taken at European level to mitigate the security risks related to the implementation of 5G networks in the community space, as well as the arguments generated by the USA and the measures taken on the Huawei subject. At the same time, the opportunity, vision and measures taken to establish a legislative and ethical framework for the use of facial recognition technologies that protect the confidentiality of personal data but also the privacy of citizens are also considered.

Keywords: 5G networks, facial recognition systems, GDPR, cyber security.

Comisia Europeană a aprobat pe 29 ianuarie 2020 setul comun de măsuri și instrumente convenite de statele membre pentru abordarea riscurilor de securitate legate de implementarea 5G. Acest lucru vine ca urmare a solicitării Consiliului European de a adopta o abordare concertată a securității 5G și a Recomandării Comisiei din martie 2019. De atunci, statele membre au identificat riscuri și vulnerabilități la nivel național și au publicat o evaluare comună a riscurilor la nivelul Uniunii Europene (UE). Prin intermediul acestui set de instrumente, statele membre se angajează să acționeze în mod comun pe baza unei evaluări obiective a riscurilor identificate și cu măsuri de atenuare proporționale. UE se opune pur și simplu interzicerii participării Huawei la construirea rețelei 5G, spunând că UE și-a definit anumite măsuri de securitate. Comisarul european pentru economie digitală, Thierry Breton a declarat Parlamentului European că excluderea Huawei nu intră în discuție, dar că vor fi aplicate controale stricte. Breton, care este fostul șef al companiei France Telecom, spunea adresându-se Parlamentului European că „*Europa nu va urma Australia, Japonia și alte câteva țări ce au decis să excludă Huawei sub presiunea administrației Trump.”* „*Scopul nu este de a introduce discriminarea, ci de a stabili reguli. Acestea vor fi stricte, exigente, dar toți operatorii pregătiți să le urmeze vor fi bineveniți în Europa, fără excludere.”*. Setul de instrumente elaborat în comun de statele membre și de Comisie, permite acestora să diversifice furnizorii pentru a evita dependența și pentru a atenua riscurile.

În data de 15 februarie 2020 Secretarul american al Apărării, Mark Esper, a declarat în cadrul Conferinței anuale de securitate de la München, că „*Washingtonul lucrează împreună cu companiile de tehnologie din Statele Unite și țările aliate pentru a dezvolta alternative la furnizorii chinezi de echipamente de rețea 5G recurgându-se deja la testarea acestora în bazele militare americane”*. În același timp, rechizitoriul de 56 de pagini întocmit de procurorii SUA este plin de exemple de comploturi ale Huawei pentru a obține secrete comerciale de la companiile americane.

https://doi.org/10.33436/v30i1y202010

Aceștia ar fi încercat să recruteze angajați din companii rivale sau profesori care lucrează la institute de cercetare pentru a avea acces la proprietatea intelectuală. De exemplu, începând cu anul 2000, inculpații ar fi luat codul sursă și manualele de utilizare pentru routerele de Internet de la o companie de tehnologie anonimă din nordul Californiei și le-ar fi încorporat în propriile routere. Ei ar fi comercializat apoi aceste routere ca o versiune cu costuri mai mici a dispozitivelor companiei de tehnologie respective. În timpul unui proces din 2003, Huawei a susținut că a eliminat codul sursă de pe routere și le-a reconfigurat, însă a șters și memoria dispozitivelor amintite și le-a trimis în China pentru a nu putea fi folosite ca probe.

Administrația Trump a precizat în repetate rânduri că are probleme de securitate națională cu privire la Huawei, inclusiv spionajul economic. Recent, președintele Trump a încercat să convingă Marea Britanie să nu mai lucreze cu Huawei pentru a le furniza echipamente în vederea construirii rețelei 5G, însă liderii britanici au făcut-o oricum. La fel și francezii și germanii. De asemenea, Huawei este acuzată că a încheiat afaceri cu companii din țări supuse unor sancțiuni americane, precum Coreea de Nord și Iran. Procurorii acuză Huawei că a ajutat guvernul Iranului "*prin instalarea de echipamente de supraveghere, inclusiv echipamente de supraveghere utilizate pentru monitorizarea, identificarea și reținerea protestatarilor în timpul demonstrațiilor antiguvernamentale, din 2009, din Teheran*". Ei spun că de zeci de ani, Huawei și-a însușit pe nedrept "*proprietate intelectuală, inclusiv de la șase companii de tehnologie din SUA, într-un efort de a crește afacerea Huawei*".

Huawei și-ar fi presat angajații să aducă informații confidențiale de la concurenți, oferind chiar bonusuri pentru "*cele mai valoroase informații furate*", se spune în rechizitoriul procurorilor americani, deși nu există dovezi în acest sens. Guvernul SUA a afirmat că a avut dovada backdoor-urilor Huawei încă din 2009, dar Uniunea Europeană declară că nu a primit astfel de informații din partea SUA și nici de la MI6 sau GCHQ. Dovezile furnizate Regatului Unit și Germaniei nu conțineau nimic nou. Oficialii americani au declarat că Huawei a construit echipamente care își păstrează în secret capacitatea de a accesa rețelele prin aceste interfețe, fără știrea operatorilor, dar nu au furnizat și dovezile în acest sens.

În final, Consiliul Național de Securitate al Marii Britanii s-a reunit și a luat o decizie cu privire la posibilitatea de a permite Huawei, gigantul chinez în telecomunicații, să ofere echipamente pentru rețeaua 5G din Marea Britanie. Această întâlnire, potrivit ”The Telegraph”, urma să fie o formalitate, miniștrii trebuind să se pronunțe în favoarea utilizării Huawei. „Nu ar trebui să existe nici o îndoială că aceasta este o decizie monumentală din toate punctele de vedere”, se spune în ”The Telegraph”. Este vorba despre importanța absolută a 5G, ce permite creșterea dramatică a volumului de date care pot fi transmise și a vitezei cu care se întâmplă acest lucru. Cu alte cuvinte, 5G va fi vital din punct de vedere economic și va gestiona cantități uriașe de date sensibile și cu caracter personal. Prin urmare, de aici vine preocuparea cu privire la permiterea pentru o companie cu legături strânse cu autoritățile chineze, să poată furniza echipamente de rețea.

Guvernul britanic a declarat că Regatul Unit trebuie să-și "diversifice aprovizionarea cu echipamente" a rețelelor de telecomunicații. Astfel, Boris Johnson a aprobat totuși doar utilizarea limitată a Huawei în rețeaua 5G din Marea Britanie, spunând că blocarea Huawei este "*exclusă*", deși a fost avertizat că este pe cale să înceapă un război diplomatic cu Donald Trump legată de planurile sale de a acorda companiei Huawei acces la rețeaua britanică de telefonie 5G. Președintele american i-ar fi spus lui Boris Johnson pe 24 ianuarie că acordarea unei astfel de permisiuni pentru Huawei ar fi o amenințare gravă la adresa securității naționale, riscând o ruptură în relațiile transatlantice, lucru care amenința să umbrească festivitățile cu ocazia Brexit, la care Boris Johnson lucra de trei ani. Dar Boris Johnson nu a cedat. Donald Trump i-a sugerat lui Boris Johnson că Marea Britanie și SUA construiesc împreună o alternativă (deținută de stat?) la Huawei, însă oficialii britanici au răspuns că va dura prea mult. Marea Britanie are o experiență îndelungată în ceea ce privește securitatea rețelelor 4G de la Huawei. Regatul Unit are în Banbury un laborator special care evaluează hardware-ul și software-ul companiei pentru riscul de securitate, doar personalul GCHQ având acces la nucleul instalației. Acest laborator publică anual un raport. Acest raport spune că în sediul de la Banbury, lângă Oxford, GCHQ a observat că din motive de reducere a costurilor, Huawei a făcut pe alocuri rabat în detrimentul securității, dar cu nicio încercare de

spionaj. Huawei a luat între timp măsuri de remediere. Marea Britanie este capabilă să monitorizeze Huawei ca o amenințare la adresa securității, dovadă fiind decizia de acum 15 ani de a folosi tehnologia în rețelele 4G și în bandă largă din Marea Britanie. Până acum, serviciile de securitate britanice nu au găsit nicio dovadă împotriva Huawei. Laboratorul din Banbury le-a criticat munca neglijentă, fapt ce a făcut ca rețeaua existentă a Regatului Unit să fie vulnerabilă în fața atacurilor cibernetice. Serviciile de informații au capacitatea de a gestiona riscul utilizării echipamentelor Huawei, decizia este cu mult mai importantă decât atât. Gordon Corera, corespondentul de securitate al BBC, a făcut un excelent rezumat al dezbaterii Huawei și a explicat faptul că serviciile britanice de securitate au fost clare în a nu dori să aibă ultimul cuvânt. Aceasta pentru că este în primul rând o decizie politică cu consecințe economice și diplomatice, precum și de securitate.

În consecință, companiei chineze i se va restricționa furnizarea de kit-uri la "părțile sensibile" și la nucleul central al rețelei în Marea Britanie. În plus, acesteia îi va fi permis să reprezinte doar 35% din kit-ul de la periferia unei rețele, care include catarge radio. Huawei va fi exclus din zonele aflate în apropierea bazelor militare și a siturilor nucleare. "*Huawei are confirmarea guvernului britanic că putem continua să lucrăm cu clienții noștri pentru a menține lansarea 5G pe drumul cel bun*", a declarat Victor Zhang, șeful firmei din Marea Britanie. "*Huawei oferă Regatului Unit acces la tehnologii de top la nivel mondial și asigură o piață competitivă*", titrează ”The Telegraph”. În mod crucial, echipamentele Huawei vor trebui să fie interoperabile cu alți furnizori, iar Marea Britanie urmează să se angajeze să colaboreze cu SUA și cu alți parteneri, pentru a stimula furnizorii occidentali și pentru a reduce dependența de Huawei.

În Franța, al doilea cel mai mare operator de telefonie mobilă, Free-Iliad, care a început să lucreze cu Nokia la prima sa rețea 5G, a declarat că dorește să lucreze și cu Huawei în viitor. Toți operatorii francezi au declarat propriului guvern că, în absența dovezilor, se opun oricărei interdicții asupra Huawei. Așadar, Franța urmează să renunțe la blocarea Huawei iar operatorii de telefonie mobilă SFR și Bouygues folosesc echipamente de rețea de la această companie, iar Orange vrea să își rezerve dreptul de a face același lucru la o dată ulterioară. Se preconizează că toți sau majoritatea operatorilor europeni de telefonie mobilă urmează exemplul Marii Britanii cu măsurile de precauție aprobate de UE. Pe de altă parte, ideea că Huawei ar spiona pentru guvernul chinez se anulează prin faptul că orice operator ce are acces sau folosește echipamentele acestora le-ar putea transmite la fel de bine toate IP-urile. IP-urile sunt cunoscute oricum de operatorii de rețea.

Nici economia nu este simplă. În prezent, dincolo de Huawei, există patru furnizori principali: Nokia - o companie finlandeză, Ericsson - o companie suedeză, Samsung - o companie sud-coreeană și ZTE - o companie chineză, pe care guvernul țării le deține parțial. Ericsson și Nokia sunt furnizorii disponibili din Vest, echipamentele lor sunt mai scumpe și, în conformitate cu ”The Telegraph”, mai puțin capabile. Bazându-se pe ele, lansarea 5G ar avea întârzieri. Acesta este de asemenea, argumentul folosit și în Franța. 5G se bazează pe rețeaua 4G existentă, astfel încât o interdicție ar însemna dezizolarea și înlocuirea echipamentelor deja utilizate. Întrucât construirea rețelei este deja în curs de desfășurare, toate aceste întârzieri s-ar adăuga la costul de excludere a Huawei. Apoi, desigur, trebuie văzută imaginea de ansamblu. SUA au reușit să interzică Huawei pentru că nu a fost un furnizor major pentru rețeaua sa 4G. Marea Britanie se află în această postură incomodă, în parte din cauza deciziei sale de acum 15 ani. “*Va persista în această dependență lăsând opțiunile Guvernului proporțional mai limitate pentru 6G?*”, întreabă ”The Telegraph”.

Este greu să distingi presiunea de la Washington în războiul său comercial cu Beijingul, dar trebuie remarcat faptul că, Congresul SUA a fost ostil Huawei cu mult înainte de Donald Trump, iar China este considerată o problemă a mai multor administrații prezidențiale americane. SUA sunt, de asemenea, conștiente de faptul că Regatul Unit nu este singura țară aflată în fața acestei decizii. De asemenea, dacă Londra nu a dat undă verde, și alte state îi pot urma exemplul. În timp ce amenințările asupra cooperării în domeniul securității par să fi scăzut, posibilitatea ca orice acord comercial cu SUA să fie afectat de această decizie, nu dispare. Există însă și o dezbatere mai largă asupra rolului economic al Chinei în lume. Beijingul construiește, de fapt, un sistem economic paralel cu cel dominat de democrațiile occidentale și își folosește influența economică

uriașă pentru a atrage națiunile în curs de dezvoltare și dezvoltate deopotrivă în acesta. China nu mai este comunistă, ci se folosește de aparatul comunist de represiune și control social, pe care l-a menținut pentru asigurarea stabilității (autoritare) țării și pentru a-și atinge obiectivele de stat. Țările din întreaga lume semnează acorduri dubioase din punct de vedere economic și politic, ca parte a inițiativei Belt and Road, iar economia globală este pe cale să se împartă în două, cu SUA pe de o parte și China de cealaltă.

În ceea ce privește discuția referitoare la 5G, ar trebui să aruncăm o privire și asupra tehnologiei de recunoaștere facială. Într-un reportaj din 3 octombrie 2019 difuzat la DIGI TV cu titlul " Sistem de recunoaştere facială, în România. Ce răspunde Poliţia celor care se tem că vor fi urmăriţi pe stradă, ca în China" și se transmite informația că "*Poliția Română își face sistem de recunoaștere facială, dar nimeni nu va fi urmărit pe stradă de camerele de luat vederi, așa cum se întâmplă în Marea Britanie sau în China*".

Tehnologiile de recunoaștere facială sunt la momentul de față un subiect de dezbatere, plecând de la diversele moduri de valorificare, până la o potențială interzicere a folosirii lor în spațiile publice. Pe măsură ce dezvoltarea și utilizarea conceptului ia amploare, un accent deosebit se pune pe analiza implicațiilor juridice și etice, pe găsirea unui echilibru între soluțiile tehnologice aflate în continuă dezvoltare și drepturile fundamentale ale cetățenilor. În acest context, jurnale precum "The New York Times" publică articole care accentuează temerea că folosirea tehnologiilor de recunoaștere facială de către poliție permite, de asemenea, accesul către viața privată a individului.

În data de 17 ianuarie 2020, BBC relata: „Comisia Europeană a dezvăluit că ia în considerare interzicerea utilizării recunoașterii faciale în zonele publice timp de până la cinci ani", iar Euroactiv informează că există proiecte în acest sens: un proiect în consultare publică cu titlul „Guidelines 3/2019 on processing of personal data through video devices" și, de asemenea, va fi publicată o Carte albă care expune cinci tipuri de reglementări pentru IA (Inteligența artificială) în spațiul european. Aceste reglementări privesc etichetarea voluntară, cerințele sectoriale pentru administrația publică și recunoaștere facială, cerințele obligatorii pentru aplicațiile cu risc ridicat, protecția cetățenilor, răspunderea și guvernanța.

Având la dispoziție aceste informații, trebuie să se analizeze dacă reglementările pot ține pasul cu ritmul rapid de dezvoltare dintr-o societate modernă sau dacă ar fi mai util să se interzică ceea ce este prea greu de reglementat. Cum să reglementezi un comportament etic dacă etica nu există fără legi, iar legile nu există fără etică. Reglementările în domeniul IA sunt mai mult decât necesare, dar dacă aceste reglementări îngrădesc cercetarea, atunci această abordare ar putea fi una total greșită.

Este lesne de observat felul în care Comisia Europeană urmărește impunerea unor obligații atât dezvoltatorilor, cât și utilizatorilor de IA modul în care creează autorități care să monitorizeze aceste reglementări, având nevoie de timp pentru găsirea unor soluții care să prevină posibilele abuzuri. Mai mult, ar trebui întreprinse cercetări asupra acestor sisteme de recunoaștere facială pentru verificarea legalității obținerii datelor cu caracter personal sau pentru evaluarea protecției și confidențialității datelor, a riscurilor și vulnerabilităților cibernetice, cât și efectele de ordin etic, juridic și social asociate.

Efortul întreprinderii unor asemenea cercetări, al stabilirii normelor de ordin juridic, tehnic și etic și a excepțiilor de la regulă va fi unul imens din toate punctele de vedere, iar costurile vor fi pe măsură. Recunoașterea facială poate fi o tehnologie de interes pentru multe domenii de activitate (securitate națională, aplicarea legii, sănătate etc.), cât și o armă care poate fi folosită în ambele sensuri.

Global se așteaptă ca până în 2022 aceste tehnologii să ajungă și să depășească 8,93 miliarde de dolari, iar până în 2025 să ajungă sau chiar să depășească suma de 10 miliarde de dolari.

Industria și din ce în ce mai multe agenții guvernamentale adoptă tehnologii 2D și 3D de recunoaștere facială, precum și alte metode, unele țări din Uniunea Europeană utilizându-le de ani buni, un exemplu de bună practică fiind Marea Britanie. Cu toate acestea sunt șanse minime ca proiectul să fie aprobat, dar interzicerea folosirii acestor tehnologii ar avea același efect ca interzicerea utilizării amprentei digitale sau a probelor ADN în anchete criminalistice. Este adevărat că într-un stat totalitar un astfel de sistem ar putea fi folosit pentru a supraveghea

opozanții sistemului, nefiind cazul Uniunii Europene. Totuși, Ungaria și Polonia au fost atacate la Curtea Europeană de Justiție în temeiul articolului 7, pentru ”comportamente nedemocratice”. Pe de altă parte, ar fi ilogic ca tehnologiile de recunoaștere facială să fie disponibile doar pentru țări cu regim totalitar, iar în țările democratice să fie interzise sau atacate în instanță.

Totodată sunt câteva aspecte care ar putea fi menționate și anume: la momentul actual nu există o bază de date internațională unitară care să conțină toate fotografiile la nivel global și care să poată fi interogată în timp real. În Marea Britanie, unde există cele mai multe camere stradale CCTV care folosesc astfel de tehnologii de recunoaștere facială, doar un anumit procent din aceste filmări este de interes pentru poliție sau alte structuri. De altfel, cele mai multe dispozitive inteligente nu recunosc ADN-ul, ci amprenta digitală sau scanarea irisului pentru a preveni utilizarea acestora de către persoane neautorizate, fiind foarte importantă protejarea confidențialității acestora. Uneori, poliția colectează probe ADN în cadrul unor anchete, chiar dacă unele dintre persoanele testate sunt declarate nevinovate, mostrele de ADN ale acestora sunt păstrate de poliție, fapt mult mai grav decât folosirea tehnologiilor de recunoaștere facială de către organele abilitate.

Cartea albă se referă atât la uzul public, cât și la cel privat al tehnologiilor de recunoaștere facială, stipulând că acestea nu se pot utiliza spre exemplu în spațiile comune ale unei clădiri de locuințe, dar se pot utiliza în incinta proprietății unei persoane. De asemenea, aceste aplicații se pot folosi cu acceptul persoanei în cauză atunci când se face check-in la conferințe sau evenimente de amploare, cu aceeași mențiune legată de confidențialitatea și protecția datelor împotriva unor eventuale intruziuni nepermise. În aceste situații folosirea unor astfel de tehnologii este importantă mai ales cu acordul participanților, într-un spațiu definit și pentru o perioadă limitată de timp.

Riscurile apar atunci când în spații publice sunt folosite astfel de tehnologii fără acceptul persoanelor vizate. Totodată, se încalcă, în unele cazuri, anumite drepturi și se ridică probleme legate de etnie, sex, vârstă, religie sau convingeri.

Se susține ideea că cei care respectă legea nu au de ce să se îngrijoreze, recunoașterea facială fiind folosită doar în scopul aplicării acesteia.

Cum ar putea fi clasificat un model IA ca produs?! Există o astfel de stipulare în Directiva NIS pentru dezvoltatorii de software, deși nu a fost testată niciodată. Este totuși o definire speculativă, dat fiind faptul că Uniunea Europeană nu acceptă modele ori software-uri în baza legislației privind brevetele. Și la unele și la celelalte există posibilitatea de a identifica, dacă este cazul, proprietarul, responsabilitatea creatorului și/sau a utilizatorului. Totuși nu este stipulată nicio modalitate clară de a solicita și dovedi dreptul de proprietate și originea și este dificil să se creeze un climat de încredere. Orice solicitare de certificare nu se va referi și la copycats, cei aflați în această situație fiind nevoiți să solicite și să-și obțină certificarea pe propria răspundere. La toate acestea se mai adaugă și legea dreptului de autor și cea legată de brevetare.

Plecând de la proiectul de Carte albă, ”The Guardian” titrează că “Uniunea Europeană ia în considerare o interdicție temporară a recunoașterii faciale”, recomandând o perioadă de evaluare a aspectelor de ordin etic și juridic în ceea ce privește folosirea sistemelor de recunoaștere facială, pentru o perioadă cuprinsă între 3 și 5 ani, perioadă în care este interzisă folosirea unor astfel de tehnologii în spațiile publice (gări, stadioane, centre comerciale etc.), pentru orice tip de actor (public sau privat). Se ridică însă un semn de întrebare asupra planurilor Germaniei de implementare a recunoașterii faciale în 134 de gări și 14 aeroporturi.

Concluzia este aceea că fiecare stat membru este responsabil pentru crearea unui cadru legislativ care să permită implementarea unor măsuri menite să protejeze cetățenii împotriva abuzurilor.

Pentru a marca Ziua protecției datelor cu caracter personal, din data de 28 ianuarie 2020, vicepreședintele Vera Jourova și comisarul Didier Reynders au emis o declarație comună: „*Datele devin din ce în ce mai importate pentru economia noastră și pentru viața noastră de zi cu zi. Odată cu introducerea tehnologiilor 5G și utilizarea inteligenței artificiale și a tehnologiilor Internet of Things, datele cu caracter personal vor fi din abundență și cu utilizări potențiale pe care probabil nici nu ni le putem imagina. Deși acest lucru oferă oportunități uimitoare, unele cazuri arată că*

avem nevoie de norme solide pentru a aborda riscurile evidente la adresa indivizilor și a democrațiilor noastre."

GDPR există de aproape 2 ani, dar confuzia și neconformitatea încă abundă. Prin puterea tehnologiei informației, orice întreprindere care vinde produse sau furnizează servicii prin internet este din punct de vedere tehnic o afacere globală. Pe scurt, dacă ai un client care locuiește într-o țară din UE și colectezi orice date de la acel client ca urmare a unei tranzacții comerciale, te supui regulilor și reglementărilor GDPR. Nu există excepții pentru dimensiunea întreprinderii sau domeniul de aplicare, ceea ce înseamnă că orice afacere cu o prezență pe internet este potențial sub rezerva acestei legi. Acesta este motivul pentru care Uniunea Europeană a pus în aplicare un nou set de reglementări menite să protejeze securitatea datelor și viața privată a cetățenilor săi.

Anchete majore cu o dimensiune transfrontalieră, care privesc mai multe persoane din mai multe state membre, sunt în curs de desfășurare. Deciziile cu privire la aceste cazuri sunt așteptate în lunile următoare. Cu toate acestea, este necesar să se intensifice aplicarea legislației, în special prin consolidarea cooperării dintre agențiile naționale de protecție a datelor. Aplicarea viguroasă și armonizarea sunt o condiție prealabilă pentru protecția eficientă a datelor cu caracter personal.

Pe 29 ianuarie 2020, Grupul de cooperare în domeniul securității informațiilor din rețeaua Uniunii Europene a lansat un set de instrumente/măsuri recomandate pentru atenuarea riscurilor de securitate în rețelele 5G. Setul de instrumente recunoaște că furnizorii cu profiluri cu risc ridicat (de exemplu, societățile cu sediul în țări terțe care nu dispun de controale și echilibre democratice) ar trebui să se confrunte cu restricții suplimentare. Acesta solicită statelor membre UE să excludă furnizorii cu risc ridicat din părțile critice și sensibile ale rețelelor lor 5G, care includ rețeaua de acces radio. Rețelele 5G vor atinge fiecare aspect al vieții noastre, inclusiv rețelele electrice, vehicule autonome, producție inteligentă, tratamente medicale și date cu caracter personal.

Având în vedere că 5G va sprijini și alte aplicații vitale, Statele Unite nu cred că este posibil să se atenueze în mod adecvat riscul prin limitarea rolului unui furnizor care nu este de încredere, la numai anumite părți ale rețelei. "*Toate părțile viitoarelor rețele 5G ar trebui considerate infrastructuri critice și fiecare țară ar trebui să dispună de măsuri pentru a proteja siguranța, securitatea și viața privată a cetățenilor care se bazează pe aceste rețele."*

Fiecare stat membru va fi responsabil pentru protejarea rețelei sale. Este greșit să credem că riscurile asociate cu instalarea de echipamente de la furnizori supuși controlului de către regimurile autoritare, cu un istoric de comportament cibernetic malign pot fi diminuate. „*Facem apel la aliații și partenerii noștri europeni să pună în aplicare recomandările UE prin adoptarea unor măsuri de securitate puternice, bazate pe riscuri, care să excludă furnizorii cu risc ridicat din toate părțile rețelelor lor 5G. Așteptăm cu nerăbdare să continuăm să lucrăm cu aliații și partenerii noștri pentru a construi un viitor 5G mai sigur, mai prosper și mai vibrant"*.

Cu alte cuvinte, "*Statele Unite salută recunoașterea de către UE a riscurilor inacceptabile pe care le prezintă furnizorii 5G care nu sunt de încredere*" și nu i-au clasificat pe Huawei și ZTE ca furnizori de neîncredere ai rețelelor 5G, ci au fost de acord să supună furnizorii de echipamente 5G la măsuri speciale de securitate.

Nu e și cazul cloud-ului. Această infrastructură este deținută exclusiv de o mână de companii. Potențialul de abuz este imens, fie că este vorba de spionaj comercial sau blocarea, încetinirea sau împiedicarea transferului datelor stocate pe infrastructură. Nimeni nu pare să se gândească la ce s-ar putea întâmpla dacă acești mamuți ar decide că este împotriva intereselor lor să aibă toate privirile ațintite asupra lor, deși ar trebui. Aproape fiecare companie modernă de tehnologie plătește pentru a-și externaliza serviciile de stocare și de calcul, fie în totalitate, fie parțial, către cloud. Această externalizare permite startup-urilor să apară cu cheltuieli de regie foarte mici și companiilor mari să își ruleze afacerile mai eficient, cu evitarea investițiilor în hardware-ul fizic. Problema este că puțini au resursele necesare pentru a reproduce infrastructura Cloud, în cazul în care proprietarii renunță brusc la clienți.

"*Contrar celor ce anunță cloud-ul ca fiind viitorul unei companii, cloud computing este aici și se întâmplă chiar acum. Întrebarea pe care trebuie să se concentreze întreprinderile nu este când, ci cum să integreze cel mai eficient cloud-ul în operațiunile lor",* spunea Shelly Kramer în data de 11 iunie 2015, în "*The Future of Cloud: Everything as a Service*".

Cei mai mari furnizori de cloud din lume sunt Amazon, Google și Microsoft. Ei au cheltuit împreună zeci de miliarde de dolari pe infrastructura centrelor de date profitând cu generozitate de pe urma acestor investiții. Având în vedere cât de critic a devenit cloud-ul pentru o mare parte a economiei, poate ar trebui să ne întrebăm dacă această infrastructură ar trebui să fie în mâinile câtorva companii de trilioane de dolari. Potențialul de abuz există în mod absolut, chiar dacă momentan nu este în interesul financiar al companiilor ce găzduiesc cloud-ul să nu mențină relații bune cu clienții lor. E greu de imaginat cum ar putea arăta un set de reglementări cu privire la neutralitatea cloud-ului. Care este interesul sectorului de înaltă tehnologie, ce este aproape în întregime în mâinile private?

BIBLIOGRAFIE

1. Cohen, Z., Bohn, K. (2019). *Trump ordered Mattis to 'screw Amazon' on Pentagon contract, according to new book*, CNN, (2020), https://edition.cnn.com/2019/10/26/politics/amazon-donald-trump-jim-mattis-pentagon-contract/index.html.
2. Directiva NIS - Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, disponibilă la adresa: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148&from=RO.
3. Esper, M. T. (2020). *Remarks by Secretary of Defense*, Conferința de securitate de la Munchen, accesat 15 februarie 2020, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2085577/remarks-by-secretary-of-defense-mark-t-esper-at-the-munich-security-conference/source/GovDelivery/.
4. *** EU eyes temporary ban on facial recognition in public places (2020) https://www.theguardian.com/technology/2020/jan/17/eu-eyes-temporary-ban-on-facial-recognition-in-public-places.
5. European Commission. (2020) *Secure 5G networks: Commission endorses EU toolbox and sets out next steps*, comunicat de presă, accesat 29 ianuarie 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123.
6. *** Facial recognition: EU considers ban of up to five years (2020), https://www.bbc.com/news/technology-51148501.
7. Kelion, L. (2020). *Huawei set for limited role in UK 5G network*, accesat 28 ianuarie 2020, https://www.bbc.com/news/technology-51283059.
8. Kennedy, M. (2020). *U.S. Prosecutors Hit Huawei With New Federal Charges*, accesat 13 februarie 2020, https://www.npr.org/2020/02/13/805821661/u-s-prosecutors-hit-huawei-with-new-federal-charges?t=1581865467345.
9. Kramer, S. (2015). The Future of Cloud: Everything as a Service, accesat 11 februarie 2020, https://fowmedia.com/future-cloud-service/.
10. *** LEAK: Commission considers facial recognition ban in AI ‘white paper’ (2020), https://www.euractiv.com/section/digital/news/leak-commission-considers-facial-recognition-ban-in-ai-white-paper/.
11. Molla, R. (2018). *Google, Amazon and Microsoft cloud businesses helped more than double spending on data centers last year. 2018 could be a record, too*., accesat 2 februarie 2020, https://www.vox.com/2018/3/15/17124300/google-amazon-microsoft-cloud-200-percent-jump-data-center-acquisitions.
12. Pompeo, M. R. (2020). *United States Welcomes the EU’s Acknowledgement of the Unacceptable Risks Posed by Untrusted 5G Suppliers*, declarație de presă, accesat pe 30 ianuarie 2020, https://www.state.gov/united-states-welcomes-the-eus-acknowledgement-of-the-unacceptable-risks-posed-by-untrusted-5g-suppliers/.
13. *Punere sub acuzare SUA against Huawei Technologies CO., LTD.*, accesat 13 februarie 2020, https://www.justice.gov/opa/press-release/file/1248961/download.

14. Rayner, G. (2020). *Boris Johnson to defy warnings from Trump and own MPs to announce Huawei will build part of 5G network*, accesat 27 ianuarie 2020, https://www.telegraph.co.uk/politics/2020/01/27/boris-johnson-defy-warnings-trump-mps-announce-huawei-will-build/?WT.mc_id=e_DM1187389&WT.tsrc=email&etype=Edi_FrB_New&utmsource=email&utm_medium=Edi_FrB_New20200128&utm_campaign=DM1187389.
15. Root, All (2019). *What the Pentagon Cloud Contract Means for Microsoft — and Other Tech Giants*, accesat 2 februarie 2020, https://www.barrons.com/articles/microsoft-wins-defense-department-cloud-contract-over-amazon-com-51572099441.
16. *** Sistem de recunoaştere facială, în România. Ce răspunde Poliţia celor care se tem că vor fi urmăriţi pe stradă, ca în China, https://www.digi24.ro/stiri/actualitate/sistem-de-recunoastere-faciala-in-romania-ce-raspunde-politia-celor-care-se-tem-ca-vor-fi-urmariti-pe-strada-ca-in-china-1195747.
17. Tamion, D. (2020). *Pas question d'exclure Huawei de la 5G en Europe, mais il y aura des règles strictes à respecter*, AFP, accesat pe 28 ianuarie 2020, https://www.universfreebox.com/article/54133/5g-pas-question-d-exclure-huawei-en-europe-mais-il-y-aura-des-regles-strictes-a-respecter.
18. Vevera, A. V., Albescu, A. R. (2018). *Factorul uman vs. Securitatea cibernetică*. Revista Română de Informatică și Automatică, Vol. 28, Nr. 4, 67-74, 2018.
19. Wheeler, C., Shipman, T. (2020). *Trump's anger over Huawei deal casts cloud on Boris Johnson's Brexit celebrations*", The Sunday Times, accesat 26 ianuarie 2020, https://www.thetimes.co.uk/article/angry-trump-casts-cloud-on-boriss-big-day-lhcs530wb?utm_source=Silverpop&utm_campaign=RA_Engagement_Global&utm_medium=email&utm_content=Huawei_M.

Florina VEVERA este consultant și analist politic, specializată în politică externă, securitate internațională și protecția infrastructurilor critice. Este licențiată în economie și drept, a absolvit mai multe studii post-universitare și de masterat și este doctor în științe militare și informații. Doamna Florina Vevera a activat atât în mediul privat, cât și cel guvernamental; a fost consilier personal al mai multor miniștri, având o experiență remarcabilă în domeniile sale de expertiză.

Este autor al mai multor volume și articole de specialitate. Portofoliul său de politică externă include arhitectura de Securitate și apărare (NATO, UE, ONU), Securitate energetică și a infrastructurilor critice, relația UE-Rusia și NATO-Rusia, securitatea bazinului Marii Negre, dar și geopolitica Orientului Mijlociu.

„Într-o vreme în care eticheta de <analist politic> tinde să se devalorizeze până la caricatură, ceea ce scrie și cum scrie Florina Vevera aduce un autentic suflu de prospețime." Celac, Sergiu (2015), Maturizarea analistului, prefață la „În lipsa globului de cristal – Provocări și Perspective", de Vevera Florina.

Florina VEVERA is an international affairs expert and consultant. She is also the autor of several volumes and articles covering geopolitics, defence and international security, foreign policy and CIP. Mrs. Vevera is currently affilieted with the IF Think Thank, with the goal of contributing to the much-needed resolution of global security challanges. Previously, she worked in the private sector and served as a counselor to many Romanian ministries, proving her remarkable know how.