Memoriu pentru informarea Comisiei pentru Afaceri Europene din Senat referitoare la problemele de siguranță a tehnologiei 5G

Stimați membri ai Comisiei pentru afaceri europene,

Deși documentul înaintat de Comisia Europeană este intitulat „*Implementarea tehnologiei 5G* ***în condiții de siguranță*** *în UE*", preocuparea care reiese din această comunicare este limitată la anumite aspecte ale siguranței cibernetice și nu abordează cum se cuvine și aspectele **siguranței naționale**, **siguranței sănătății populației și a ecosistemului viu**, **siguranței mediului înconjurător, siguranței socio-economice și drepturile fundamentale, inclusiv dreptul la viață privată.** Prin urmare, „setul de instrumente propus spre a fi pus în aplicare" este parțial, nicidecum „cuprinzător", nu corespunde necesităților reale, multiple, generate de implementarea acestor tehnologii, nu asigură, așa cum susține Comisia, nici *„protejarea economiilor, a societăților și a proceselor noastre democratice"* și nici *„o transformare digitală de natură să inspire încredere pentru toți cetățenii UE"*.

Punctul nostru de vedere include și aspectele **siguranței sănătății, siguranței ecologice, siguranței naționale, siguranței socio-economice și a siguranței cibernetice și vă solicităm răspunsuri și garanții,** în calitatea dumneavoastră de co-responsabili cu decizia implementării tehnologiei 5G în România.

Planul *Setului de Instrumente al UE* conține propuneri referitoare la eventuale avantaje economice și se referă doar la riscurile de ordin cibernetic și la cele legate de protecția datelor, fiind vizați în principal operatorii din industria telecom. Considerăm foarte îngrijorător faptul că sunt ignorate total atât riscurile la care sunt expuși utilizatorii/membrii Uniunii Europene cât și impactul acestei tehnologii asupra mediului și ecosistemului în care trăim cu toții. În plus, în cazul României, lipsește infrastructura necesară aplicațiilor tehnologiei 5G: autostrăzi, transport, școli dotate la standarde europene, infrastructura spitalicească, în special în zonele rurale sau orașe mai mici etc.

De asemenea, implementarea tehnologiei 5G nu poate fi realizată fără consultarea largă a cetățenilor, pe baza unor dezbateri reale, mediatizate la nivel național, la care să participe și reprezentanți ai societății civice cu experiență în domenii relevante, precum sănătate, IT, biologie, biochimie, drept constituțional și siguranță națională. În acest sens considerăm că **este obligatorie respectarea prevederilor Convenției AARHUS**, transpuse în România prin Legea nr. 86/2000, care prevede accesul la informații, organizarea și susținerea dezbaterilor publice ample, cu subiecte de interes pentru cetățeni, participarea la luarea deciziilor etc.

Este esențială și informarea pe subiect, în timp util, a societății civice, referitoare la documentele UE, pentru ca reprezentanții acesteia să-și poată prezenta opinia avizat.

Parcurgând documentul *Comunicarea Comisiei Europene referitoare la implementarea rețelelor 5G în condiții de siguranță în UE* se observă caracterul ambiguu, birocratic, și, în ultimă instanță, inacceptabil - având în vedere că decizia implementării acestei tehnologii ar produce efecte ireversibile. Înainte de implementarea tehnologiei 5G este necesar să se stabilească *cu precizie*, pe baza unor argumente solid justificate, instrumente și măsuri de *prevenire a tuturor riscurilor* - și nu doar de "atenuare a riscurilor" de natură cibernetică.

Suntem de acord că nici o tehnologie nu este lipsită în totalitate de riscuri. Cu toate acestea, sunt inacceptabile și profund îngrijorătoare afirmațiile de genul: "pentru fiecare din domeniile de risc identificate în evaluările coordonate la nivel de UE a riscurilor sunt prevăzute planuri de atenuare a riscurilor bazate pe măsuri cu eficacitate maximă" - Comunicarea Comisiei Europene, pag. 5. Societatea civică dorește nu numai măsuri pentru "atenuarea riscurilor", ci și prevenirea acestora și cere explicații referitoare la cuantificarea realistă a ceea ce înseamnă "eficacitate maximă"!

În *Comunicarea Comisiei Europene* se afirmă că până la data de 30 aprilie 2020 fiecare stat membru UE trebuia să "întreprindă acțiuni concrete și cuantificabile pentru punerea în aplicare a setului de măsuri cheie recomandate de UE"! Este necesar să cunoaștem care sunt măsurile recomandate de UE legate de acest subiect și ce dorește România să raporteze?

În afara celor menționate, vă adresăm dvs. și Comisiei Europene următoarele întrebări, argumentate, legate de aspectele de risc și securitate referitoare la implementarea tehnologiei 5G:

I. SIGURANȚA SĂNĂTĂȚII

1. Ce entitate economică sau autoritate a statului va oferi și va avea **responsabilitatea juridică** în cazul daunelor asupra sănătății populației și a ecosistemelor produse de dispozitivele de comunicație radio, parte integrantă din infrastructura rețelelor 5G, de exemplu produse de dispozitive de tip "small cell" instalate la distanțe foarte mici (metri sau zeci de metri) față de locuințele oamenilor, școli, spitale etc.? Amintim inclusiv că firmele de asigurări nu acoperă bolile generate de poluarea electromagnetică.

2. Ce entitate economică sau autoritate a statului va oferi și își va asuma **responsabilitatea financiară** pentru daunele, incendiile, **afectarea sănătății**, **devalorizarea proprietăților din cauza învecinării cu** stațiile de radio emisie/antene?

3. Care sunt **studiile** care atestă clar că tehnologia 5G este sigură din punctul de vedere al efectelor asupra sănătății oamenilor și nu prezintă impact negativ asupra mediului?

4. De ce Comisia amintește atât de puțin (o singură propoziție) despre problemele legate de sănătate? De ce Comisia Europeană nu definește **criteriul „relevanței"** pentru "aspectele sănătății" și pentru "cooperare cu organizații internaționale"? Și cât de democratic și transparent este acest criteriu din moment ce Comisia Europeană, dar și Statul Român refuză să actualizeze standardele de protecție a populației la expunerea la radiații neionizante (emisiile ambientale de radiofrecvență ale rețelelor de telecomunicații mobile)? Aceste standarde sunt mai vechi de 20 de ani și neactualizate, în contextul tehnologiei din ce în ce mai prezente.

5. De ce nu promovează și nu alocă Comisia Europeană și/sau Statul Român fonduri pentru cercetarea și investigarea impactului acestor noi tehnologii asupra sănătății omului și a mediului înconjurător, înainte de luarea oricărei decizii ce obligă la implementarea lor?

6. La dezbaterile publice organizate de societatea civică din România, medicii au prezentat - din practica curentă - cazuri ale unor pacienți, în majoritate tineri, ce suferă de sindromul de hipersensibilitate electromagnetică, cărora li s-a recomandat ferm schimbarea locului de muncă. O dovadă clară a impactului negativ al radiațiilor de radiofrecvență asupra sănătății este faptul că diverși funcționari, inclusiv angajații din Parlamentul României, au **spor de periculozitate datorită unei antene** amplasată pe clădirea instituției. După aceeași logică, întrebăm: **ce sporuri ar trebui să fie plătite tuturor românilor care sunt afectați de antenele de telecomunicații** amplasate pe blocuri, spitale, școli și pe alte clădiri publice?

Vedeți argumentarea "SIGURANȚA SĂNĂTĂȚII" de la pag. 7.

II. DATELE ȘI INFORMAȚIILE DE SIGURANȚĂ NAȚIONALĂ

1. Ce măsuri vor lua și ce condiții vor impune autoritățile Statului Român operatorilor de telecomunicații pentru garantarea securității datelor de interes național, economic și militar care tranzitează aceste rețele, din ce în ce mai vulnerabile?

2. Cum va fi gestionată siguranța națională referitoare la informațiile transmise prin, și stocate în rețelele 5G, în condițiile în care tehnologia aceasta este încă una **experimentală, nereglementată, insuficient testată și invazivă?**

Vedeți argumentarea "SIGURANȚA NAȚIONALĂ" de la pag. 10.

III. SIGURANȚA SOCIO-ECONOMICĂ

1. De ce, din considerente în majoritate economice, e promovată și chiar impusă de către Uniunea Europeană implementarea tehnologiei 5G, în condițiile în care este demonstrat științific și statistic faptul că nu viteza de transmitere a datelor și nici latența conexiunii nu sunt factorii determinanți pentru prosperitatea comunităților?

2. Care sunt garanțiile pe care Comisia Europeană și Statul Român ni le oferă că în Europa și/sau în România nu vor crește șomajul și excluziunea socială, generate de automatizări și de implementarea 5G?

3. Care sunt programele și fondurile alocate de Comisia Europeană și de Statul Român pentru a preveni și proteja Europa și statele membre de impactul pierderii de locuri de muncă, generat de implementarea 5G?

Vedeți argumentarea "SIGURANȚA SOCIO-ECONOMICĂ" de la pag. 12.

IV. SECURITATEA CIBERNETICĂ

1. Cum veți măsura implementarea și respectarea, de către operatorii de telecomunicații mobile, a celor mai bune practici în domeniul securității datelor personale din rețelele 5G? După cum o demonstrează atâtea evenimente celebre de *hacking* bancar și politic*,* este clar faptul că nici cele mai bune metode și practici de securitate din prezent nu sunt suficiente pentru asigurarea securității sistemelor cibernetice.

2. Ce măsuri concrete vor impune Comisia Europeană și autoritățile Statului Român operatorilor de comunicații electronice mobile, pentru garantarea securității cibernetice a aplicațiilor **IoT** (*Internetul lucrurilor*) ce folosesc aceste rețele?

3. Ce autorități ale Statului Român au sau vor avea capacitatea să evalueze riscurile de securitate cibernetică ce pot apărea în rețelele publice mobile de comunicații electronice 5G? Cine va plăti imensele daune în cazul unor

consecințe grave de natură economică și cum se va face aceasta transparent și public?

4. Ce autorități ale Statului Român vor putea fi **trase la răspundere (civil și penal)** în cazul în care va lipsi capacitatea de a reacționa rapid, prin eliminarea imediată a breșelor de securitate cibernetică depistate în rețelele publice mobile de comunicații electronice 5G?

5. Prin specificul arhitecturii rețelelor 5G, echipamentele folosite sunt foarte descentralizate și expuse atacurilor. Din acest motiv, securitatea lor cibernetică este foarte greu de realizat. Ce garanții oferă Comisia Europeană și autoritățile Statului Român cu privire la vulnerabilitățile de securitate ce țin de însăși modificările arhitecturale ale rețelelor și tehnologiei 5G?

Vedeți argumentarea "SECURITATEA CIBERNETICĂ" de la pag. 16.

V. SIGURANȚA ECOLOGICĂ

1. Dat fiind că echipamentele 5G generează o cantitate foarte mare de deșeuri electronice, întrebăm: pot actualele capacități de reciclare să gestioneze un asemenea aflux de deșeuri?

2. Ce garanții ni se oferă ca România să nu devină un imens depozit de deșeuri electronice?

Vedeți argumentarea "SIGURANȚA MEDIULUI ÎNCONJURĂTOR" de la pag. 22.

VI. ABSENȚA TRANSPARENȚEI ÎN IMPLEMENTAREA TEHNOLOGIEI 5G ÎN ROMÂNIA

Societatea civică a făcut în ultimii doi ani numeroase demersuri pentru ca autoritățile să facă publice acțiunile, deciziile și documentele ce stau la baza *Strategiei 5G pentru România*. Cu toate acestea, singurul răspuns al autorităților a fost un adevărat ping-pong al responsabilităților, de la o instituție la alta (ANCOM, SGG, Ministerul Comunicațiilor, Camera Deputaților etc.). Mai mult, Ministerul Sănătății și Institutul Național de Sănătate Publică, în ciuda atribuțiilor legale pe care le au, nu vor să-și asume niciun rol, nu vor să facă studii de specialitate, nu vor să se angajeze în niciun fel în clarificarea multiplelor probleme și riscuri de sănătate generate de tehnologia 5G. În particular, Ministerul Sănătății a sfidat nu doar apelurile și petițiile noastre, ci și pe cele venite din partea altor instituții ale statului român, inclusiv din partea unor jurnaliști. Această atitudine demonstrează că, în numele beneficiilor

economice ale corporațiilor, factorii politici decidenți eludează legea și drepturile omului (începând cu dreptul esențial la sănătate).

1. Ce veți face pentru a determina Ministerul Sănătății să-și ia atribuțiile în serios și să facă studiile necesare privind sănătatea publică vs. radiațiile electromagnetice neionizante?

2. Ce veți face pentru ca Ordinul Ministrului Sănătății nr. 1193/29.09.2006, să fie anulat, deoarece:
   a. este complet învechit;
   b. nu se referă la actualele tehnologii 5G (deși se aplică și în cazul lor);
   c. nu respectă trendul internațional. Trebuie ca România să se alăture numeroaselor țări care au actualizat, în mod responsabil (în scopul protejării sănătății propriilor populații), pragul de valori maxime admisibile pentru radiațiile electromagnetice.

3. Ce măsuri veți lua în calitate de parlamentari pentru ca autoritățile competente să ne răspundă în mod adecvat la întrebări și să facă dezbateri publice pe toate subiectele legate de tehnologia 5G?

Referitor la pct. VI. 2. c. de mai sus - actualizarea pragurilor valorilor maxime admise - menționăm următoarele: valorile maxime admisibile trebuie să fie fundamentate pe durata expunerii, pe frecvență, pe lungimea de undă, pe modulația și mixarea frecvențelor, pe forma undelor, pe lățimea pulsului precum și pe alte proprietăți semnificative din punct de vedere biologic. Chiar și cu actualele metodologii și standarde, limitele admise de expunere la EMF în anumite state ca Polonia, Bulgaria, China, Rusia, Franța și Belgia (cu limite în unele regiuni chiar mai mici, cum ar fi în Paris și Bruxelles) sunt stabilite la valori de până la ZECE ORI MAI STRICTE față de valorile admise în standardul internațional ICNIRP (acesta fiind valabil încă în România, conform Ordinului Ministrului Sănătății nr. 1193/2006). Această actualizare, prin reducere semnificativă și rațională a valorilor maxime admisibile, este necesară tocmai pentru a diminua impactul negativ al rețelei de telecomunicații asupra populației și mediului. Limitele expunerii publicului la radiațiile electromagnetice în țările menționate mai sus sunt:

Bulgaria	6.13 V/m;
Polonia	6.14 V/m;
Belgia - Bruxelles	6 V/m;
- Flandra	20.6 V/m;
- Valonia	3 V/m;
China	12 V/m;
Rusia	25 V/m;

în timp ce:

România	**61 V/m !!!**

SIGURANȚA SĂNĂTĂȚII

Singura menționare în această comunicare cu privire la siguranța sănătății și mediului este:

Comisia va continua să sprijine pe deplin instalarea cu succes a tehnologiei 5G în UE, inclusiv prin colaborarea cu statele membre și cu părțile interesate pentru a valorifica oportunitățile oferite de tehnologia 5G. Se va acorda atenția cuvenită aspectelor ***relevante*** *legate de sănătate, pe baza principiului precauției, în cooperare cu organizațiile internaționale* ***relevante*** *și cu comunitatea științifică*. ***Comunicarea Comisiei Europene***

Este o exprimare ambiguă și inacceptabilă!

Deși există mii de studii de calitate ce demonstrează influența negativă a radiațiilor electromagnetice neionizante asupra biologicului, Comisia nu a promovat programe de finanțare pentru realizarea de studii, cercetări și inovări în privința impactului tehnologiei 5G la adresa biologicului, așa cum a finanțat în *extenso* cercetarea și implementarea 5G. Menționăm că **Organizația Mondială a Sănătății a început studierea riscurilor ce pot proveni din expunerea la câmpuri radio.** Organizația Mondială a Sănătății are în derulare un proiect de evaluare a efectelor câmpurilor electromagnetice asupra sănătății. În luna noiembrie 2019 a lansat procedura de selecție pentru atribuirea contractelor de cercetare pentru studii care să analizeze și să sintetizeze dovezile existente până în prezent. Aceasta înseamnă că în curând vom avea primele rezultate ale unor studii medicale actualizate, care vor arăta fără echivoc efectele nocive asupra sănătății ale undelor radio cu frecvențe în spectrul 5G.

Cum ar putea să inspire încredere cetățenilor UE aceste planuri și ambiții, în mare măsură economice, din moment ce însăși Comisia Europeană se declară într-un mod vădit dezinteresată față de sănătatea *acestei chestiuni și arată în concluziile sale pericolele pe care emisiile de tip telefonie mobilă, precum telefonul mobil, emisiile UMTS-Wifi-Wimax-Bluetooth și telefonul fix "DECT" le pot avea pentru sănătate;*

22. constată că limitele de expunere la câmpurile electromagnetice fixate pentru public sunt învechite, având în vedere că nu au fost adaptate de la Recomandarea 1999/519/CE a Consiliului, din 12 iulie 1999, privind limitarea expunerii publicului la câmpurile electromagnetice (0 Hz la 300 GHz) și în mod evident nu țin seama de evoluția tehnologiilor informației și comunicațiilor și nici de recomandările preconizate de Agenția Europeană pentru Mediu sau de normele de emisie mai exigențe luate, de exemplu, de Belgia, Italia sau Austria și nu țin seama de grupurile vulnerabile, cum ar fi femeile însărcinate, nou-născuții și copiii;

23. solicită astfel Consiliului să modifice Recomandarea 1999/519/CE, pentru a ține seama de cele mai bune practici ale statelor membre și a stabili astfel valori limită de expunere mai stricte, pentru totalitatea echipamentelor emițătoare de unde electromagnetice cu frecvența cuprinsă între 0,1 MHz și 300 GHz;"

Sursa: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0410+0+DOC+XML+V0//RO.

Mai mult, în 2011 Consiliul European emite **Rezoluția 1815 CE** conform căreia **aplicarea principiului precauției** în privința radiațiilor electromagnetice emise de echipamentele wireless să se realizeze printr-o serie de măsuri precum: înăsprirea limitelor de expunere, evitarea amplasării antenelor/echipamentelor în preajma copiilor, consultarea populației de către autorități și multe altele, măsuri menite a ne proteja o dată cu introducerea pe piață a rețelei 4G.

Sursa: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17994.

Deși există aceste reglementări legislative cu măsuri clare de prevenire și siguranță a populației, **Comisia Europeană, autoritățile statului român** (ANCOM, Ministerul Sănătății, Ministerul Mediului etc.) și **operatorii și producătorii telecom nu le îndeplinesc**! Ba mai mult, respectivii forțează, accelerând implementarea tehnologiei 5G, care este de zeci de ori mai poluantă electromagnetic decât cea deja existentă (implică trilioane de conexiuni, milioane de antene, zeci de mii de sateliți spațiali etc.).

Deși Comisia Europeană impune statelor membre implementarea 5G, la nivelul Parlamentului European **abia în februarie 2020** s-a constituit, cu o lentoare birocratică antologică, un grup de analiză al consecințelor și riscurilor asupra sănătății. Aceasta a survenit doar sub presiunea **sesizărilor multiple, făcute de-a lungul a mai multor ani de zile, de către comunitatea științifică mondială**.

Sursa:
https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646172/EPRS_BRI(2020)646172_EN.pdf.

Acest mod de operare, profund birocratic și iresponsabil al autorităților europene și naționale, care arată lipsa preocupării reale pentru protecția sănătății oamenilor și a mediului, constituie publică? Este de-a dreptul ipocrită pretenția aplicării *principiului precauției* atunci când, pentru o tehnologie a secolului 21, Comisia urmează standarde de siguranță din anul 1999, învechite, extrem de permisive și reducționiste! Se consideră „relevant" **doar impactul termic al radiațiilor** neionizante, în timp ce comunitatea științifică internațională semnalează de zeci de ani și demonstrează printr-o baza largă de cunoștințe, formată din mii de studii, că aceste radiații neionizante, emise de echipamentele telecom wireless au **impact sever, cu caracter non-termic, asupra celulei vii**. Din aceste motive crește incidența mai multor boli în rândurile utilizatorilor wireless și dispariția unor specii, ca urmarea a acestor radiații.

Încă din anul 2008 Parlamentul European a solicitat Comisiei Europene revizuirea standardelor si, în mod bizar, **nici până în prezent CE nu a întreprins măsurile necesare siguranței sănătății.** Ce încredere mai pot avea cetățenii în intențiile CE?

"*Parlamentul European este extrem de preocupat de raportul internațional Bio-Initiative privind câmpurile electromagnetice, care sintetizează mai mult de 1 500 de studii consacrate*

motivul principal pentru care nu putem avea încredere în măsurile propuse și considerăm necredibile afirmațiile generice, fără conținut, pe acest subiect. **Solicităm să ni se prezinte un studiu de impact asupra sănătății** pe termen scurt și îndelungat și consecințele tehnologiei 5G asupra mediului și ecosistemelor asociate, precum și **garanții ferme, înainte de a implementa această tehnologie pe spectrul radio românesc**. Acest spectru este o resursă naturală limitată și este proprietatea publică a poporului român. Indiferent ce prognoze/premise economice se vehiculează, **solicităm aplicarea principiului precauției și suspendarea oricăror demersuri** care să permită operabilitatea tehnologiei 5G (inclusiv testarea acesteia pe teritoriul României), până când vor exista garanțiile că aceasta este sigură din toate punctele de vedere, inclusiv din cel al sănătății publice.

Deoarece autoritățile nu monitorizează corespunzător nivelul radiațiilor și poluarea electromagnetică din România, prezentăm câteva măsurători independente ale radiațiilor emise de echipamentele telecom în Sibiu și în București:

https://www.facebook.com/Stop5GSibiu/videos/207332890622447/ (Stația de metrou Izvor, București);

https://www.facebook.com/Stop5GSibiu/videos/250719772677050/ (Str. Bieltz, Sibiu).

Raportarea tuturor măsurătorilor efectuate se află aici:

https://www.google.com/maps/d/u/0/viewer?hl=ro&mid=1SyNtPe8lZTWyqDFNnicyrXhEUx9bLr25&ll=46.42164430506008%2C22.321165382819025&z=7&fbclid=IwAR2Z0tBa4no3LuY7neFe0JKuZTzGtJUw-lbA9RFjXRdS4B_IYkdlUh5oL_8.

Din aceste măsurători (care, conform bornelor-marker roșii din linkul de mai sus, ajung și la **276 mW/m^2 în Sibiu** sau la **368 mW/m^2 în București**), se observă că **nivelul este cu mult peste cel recomandat** de Rezoluția 1815 CE și de studiul ***STOA*** *(Science and Technology Options Assessment - Organization Valuation Sciences and Technologies of the European Parliament*), **efectuat de Parlamentul European, ale cărui limite recomandate sunt de 0,1 mW/m^2** (100 μW/m^2). Așadar, avem în România valori ale intensității câmpului electromagnetic de **2760 până la 3680 de ori mai mari decât cele admise în studiile Parlamentului European**!

Sursa pentru studiul STOA al Parlamentului European: https://www.home-biology.com/images/emfsafetylimits/EuropeanParliamentSTOA.pdf.

Pentru a se vedea că limita la care ne raportăm, indicată de Parlamentul European, aceea de 0,1 mW/m^2 este una deja permisivă pentru industria telecom, indicăm aici un tabel din care se observă clar că alte instituții internaționale recomandă limite mult mai stricte (chiar de zeci de ori mai mici).

Sursa: https://www.home-biology.com/electromagnetic-field-radiation-meters/safe-exposure-limits.

Referitor la radiațiile emise de echipamentele wireless, legislația românească reglementează sporul de toxicitate al angajaților statului, prin Legea 153/2017 privind salarizarea personalului plătit din fonduri publice, care se aplică funcționarilor publici, respectiv Parlamentul, Administrația Prezidențială, autoritatea judecătorească, Guvernul, Ministerele, Consiliul Concurenței, Consilii locale etc. Aceasta deși nivelele măsurate de ANCOM în instituțiile respective nu depășesc standardele românești de limitare a expunerii la radiații neionizante. Avem de-a face cu un dublu standard deoarece, în timp ce toată populația României este încadrată în normele naționale, foarte permisive (**61 V/m** și **10 W/m^2**), o parte din funcționarii publici sunt încadrați la alte standarde, primind sporuri în bani pentru aceasta!

Sursa: http://stop5gromânia.ro/radiatiile-antenelor-pentru-noi-sigure-pentru-angajatii-statului-toxice/.

SIGURANȚA NAȚIONALĂ

d) dacă o parte din noile scenarii de utilizare avute în vedere pentru 5G ajung să se concretizeze, rețelele 5G vor ajunge să reprezinte o parte importantă a lanțului de aprovizionare al multor aplicații informatice critice și, ca atare, nu numai că va exista un impact asupra cerințelor în materie de ***confidențialitate și protecție a datelor*** *cu caracter personal,* ***dar integritatea și disponibilitatea acestor rețele vor deveni la rândul lor preocupări de importanță majoră pentru securitatea națională*** *și o provocare majoră în materie de securitate din perspectiva UE.*

Comunicarea Comisiei Europene *(extras din Raportul ENISA)*

Reiteram faptul că strategiile „*Digital Single Market*”, „*Un plan de acțiune privind 5G în Europa*” „*Conectivitate pentru o piață unică digitală competitivă - către o societate europeană a gigabiților*” etc. și obiectivele „ambițioase” ale Comisiei Europene nu sunt obligatorii Statelor membre. României ii revine dreptul suveran de a decide în baza studiilor de impact și a propriului context socio-economic, dacă este oportun sau nu să implementeze pe teritoriul

său o tehnologie **încă experimentală, nereglementată, insuficient testată, invazivă și nesigură.**

În plus, reamintim faptul că furnizorii rețelelor de telecomunicații sunt **entități private străine** care urmăresc în primul rând profitul economic inclusiv prin a-și diminua costurile de implementare. Rețelele de telecomunicații mobile nu sunt de utilitate publica și **nu pot fi puse înaintea siguranței și interesului național**. Transformarea unui demers economic și tehnologic într-un demers „strategic" pentru țara nu e fundamentată, nu este democratica și nici constituțională. Nu poți facilita legislativ și/sau conferi puteri sporite unor birocrați și tehnocrați, indiferent că o recomanda Uniunea Europeană, deoarece aceasta tehnologie pune în pericol însăși siguranța națională a României.

Fostul comandant al trupelor NATO din Europa, General (r.) James Jones a afirmat ca: „*Cred că cea mai mare **amenințare nu ține atât de sisteme de arme, cât de tehnologie** precum tehnologia 5G sau inteligența artificială și modul în care autocrații se vor folosi de tehnologie să penetreze democrațiile noastre. Asta e amenințarea momentului. **Aspectul de siguranță la tehnologia 5G trebuie să fie cel mai important***" Sursa: https://tinyurl.com/u388l53.

Urmărind "*Setul de instrumente cu măsuri de atenuare a riscurilor al UE, 29 ianuarie 2020*" Sursa: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group, este evidenta preocuparea și promovarea de către Comisia Europeană a sporirii puterii unor autorități care în mod constant au demonstrat cetățenilor europeni că răspund nevoilor unor entități **transnaționale (corporațiilor) și nu cetățenilor**. Tehnologia 5G prin facilitățile oferite, dar mai ales prin facilitățile legislative promovate la nivel european și național au un profund caracter abuziv, nedemocratic încălcând multiple tratate internaționale, constituții și legislații primare. Aceste aspecte au fost prezentate de noi pe larg în memoriile anterioare, înaintate autorităților române (*e.g.,* Memoriul Stop 5G etc.)

Nu putem să nu remarcăm în Comunicarea Comisiei Europene insistenta preocupare legată de agenții economici, de aspectul „furnizorilor cu profil de risc ridicat" și de aspectul „*dependență majoră de un furnizor unic*". Arhitectura și protocolul rețelei 5G prezinta nenumărate vulnerabilități care se regăsesc la **toți furnizorii** indiferent că sunt sau nu cunoscuți ca fiind "cu risc ridicat". Aceasta abordare exclusiv economica ignora securitatea naționala a statelor.

*La rândul său, acest lucru va face să crească numărul de căi de atac care ar putea fi exploatate de factorii de amenințare, în special de **actori statali sau sprijiniți de stat** din afara UE, din cauza capacităților lor (în ceea ce privește intențiile și resursele) de a efectua atacuri împotriva rețelelor de telecomunicații ale statelor membre ale UE, precum și gravitatea potențială a impactului unor astfel de atacuri.* ***Comunicarea Comisiei Europene***

Evenimentele recente în care înregistrări ale unor convorbiri telefonice purtate de demnitari români sunt pe internet, sau în care diverse tipuri de date sensibile sunt făcute publice (*e.g.,*

https://soundcloud.com/român-drept), sursa acestor înregistrări fiind chiar furnizorii actuali ai rețelei de telecomunicații. Aceasta este una cele mai scandaloase dovezi ale faptului că entități străine permit accesul serviciilor de informații străine la datele transferate în rețelele lor.

Astfel, ne punem problema că toate datele care trec prin aceasta viitoare rețea 5G , inclusiv date cu caracter militar/secret de stat/siguranța națională pot ajunge pe mâinile unor entități, indivizi sau centre de inteligenta artificiala potrivnice României, indiferent că acestea sunt europene sau non-europene.

Cadru privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare (Setul de instrumente pentru diplomația cibernetică)**: În cazul unor activități cibernetice răuvoitoare care amenință integritatea și securitatea UE, statele membre sunt încurajate să utilizeze măsurile relevante din cadrul politicii externe și de securitate comune care fac parte din Setul de instrumente pentru diplomația cibernetică al UE (inclusiv, dacă este necesar, măsurile restrictive), pentru a încuraja cooperarea, a facilita atenuarea amenințărilor și a influența comportamentul potențialilor agresori.* ***Comunicarea Comisiei Europene

Comisia Europeană pune problema diplomației cibernetice doar în raport cu atacurile la integritatea și securitatea UE, nu și la atacurile ce pot veni chiar din interiorul UE la integritatea și securitatea unui stat membru cum este România.

Setul de instrumente face posibilă o abordare comună a UE în domeniul securității cibernetice a rețelelor 5G, sprijinind coerența la nivelul întregii piețe comune prin politici ale UE și prin coordonare la nivelul întregii UE, precum și exercitarea competențelor statelor membre, în special în ceea ce privește securitatea națională. ***Comunicarea Comisiei Europene***

În mod explicit Comisia pune în situație de vulnerabilitate sporită statele membre încercând să impună aceste tehnologii, lăsându-le acestora responsabilitatea și sarcina exercitării competentelor pe securitate națională care este pusă efectiv sub asediu de însuși protocolul și arhitectura acestor tehnologii. La final însă, cei care vor suporta consecințele sub toate aspectele sunt cetățenii statelor naționale membre, cărora li se impune aceasta tehnologie fără a fi consultați în conformitate cu convențiile internaționale și legislațiile naționale!

SIGURANȚA SOCIO-ECONOMICĂ

Analiza Academiei Române:

Sistemele de comunicații implementează generația 5G, serviciile web avansează rapid către generația Web 3.0, iar sistemele de fabricație au atins generația "Industry 4.0". În același timp, odată cu apariția de noi meserii menite să compenseze dispariția unor locuri de muncă, ***apar***

***vulnerabilități majore pentru siguranța și protecția vieții private a cetăţenilor și chiar influențe asupra stării de sănătate și comportamentului individului**, în contextul aplicării pe scară largă a tehnologiilor emergente, care tind să înlocuiască operatorii umani și să modifice deprinderile dobândite de-a lungul secolelor de evoluție umană*."

Sursa: https://acad.ro/mediaAR/com2019/c1016-ManifestEraDigitala.htm.

DIGITALIZAREA EUROPEI PRIN IMPLEMENTAREA 5G **NU DETERMINĂ CREȘTEREA NUMĂRULUI DE LOCURI DE MUNCĂ, CI DIN CONTRĂ, CREȘTE ȘOMAJUL.**

Conform studiului "*Industry 4.0 ca Vinovat al Șomajului (**Industry 4.0 as the Culprit of Unemployment**) - 2017*" prezintă și atrage atenția asupra **iminenței pierderii unui număr semnificativ de locuri de muncă** ca urmare a avansului digitalizării și automatizării sarcinilor îndeplinite de lucrători umani:

„Riscul cu care ne confruntăm în viitorul apropiat este șomajul mai mare în anumite zone, afectând în principal locuri de muncă cu un nivel scăzut de calificare. Tendința de a merge mai departe și a veni cu noi aplicații, mașini și tehnologii va înflori în continuare, iar iminentele pierderi de locuri de muncă trebuie abordate în mod serios. Este clar că persoanele fără locuri de muncă nu pot produce venituri și, mai mult, ele pun o presiune mai mare asupra sistemului social. Banii plătiți șomerilor trebuie găsiți undeva, iar acest lucru este de obicei rezolvat printr-o povară fiscală mai mare. Sarcina este să ne gândim la aceste amenințări și să ne adaptăm la ele cât mai repede posibil, pentru a asigura un viitor mai bun pentru omenire."

Sursa: http://www.cutn.sk/Library/proceedings/km_2017/PDF_FILES/09_Matovcikova-71-78.pdf.

Cu același tip de concluzii și prezentând aceeași tendință, studiul intitulat "*Efectele Digitalizării asupra Șomajului și Antreprenoriatului (**The Effects of Digitalization on Employment and Entrepreneurship**) - 2018*" prezintă **antreprenoriatul ca singură pseudo soluție, inclusiv aceea a antreprenoriatului de tip forțat**, în sensul în care decizia de a urma calea antreprenoriatului va rămâne singura opțiune pentru categoria de lucrători umani disponibilizați datorită avansului tehnologic, al digitalizării și automatizării, această forțare neputând în realitate garanta în niciun fel veniturile și profitul necesare unui nivel de trai decent și sănătos.

"*Demonstrăm că noul val de digitalizare și Inteligență Artificială (AI) are deja un impact asupra pieţelor muncii. Arătăm că lucrătorii răspund schimbându-și ocupația sau devenind antreprenori. Cu toate acestea, a doua opțiune nu este disponibilă celor mai vulnerabili lucrători în ocupații cu cel mai mare risc de automatizare, în special femeile. Politica publică ar trebui să ajute acești lucrători să se adapteze și să dobândească noi abilități necesare pentru a rămâne productivi. Pe celălalt capăt al spectrului, arătăm, de asemenea, că digitalizarea creează noi oportunități pentru antreprenorii orientați spre creștere, care fac trecerea de la angajarea plătită la antreprenoriat, chiar și fără a avea un risc propriu ridicat de automatizare profesională.*"

”*O altă constatare importantă care a fost în mare parte ignorată în discuțiile despre viitorul ocupării forței de muncă este că riscul digitalizării afectează și tranzițiile individuale către antreprenoriat. Arătăm că tranzițiile în antreprenoriatul încorporat, care este legat de antreprenoriatul productiv în ceea ce privește orientarea spre creștere și crearea de locuri de muncă, tind să apară mai probabil din ocupațiile mai degrabă „sigure”, cu un nivel scăzut de risc de automatizare. Tranzițiile către antreprenoriat încorporat, care este legat de antreprenoriatul de necesitate, apar cel mai probabil din ocupații cu nivel mediu de risc de automatizare și sunt cel mai puțin probabil din ocupații cu risc foarte mare sau foarte mic. Astfel, deși pentru lucrătorii cu ocupații cu risc mediu de automatizare, antreprenoriatul încorporat este utilizat ca o cale de evadare, antreprenoriatul nu pare a fi o opțiune viabilă pentru lucrători, în special pentru femei, în ocupații cu riscuri ridicate de automatizare. Acest lucru este plauzibil, deoarece munca independentă nu este sustenabilă dacă mașinile digitale și AI vor putea în curând să îndeplinească aproape toate sarcinile pe care acești lucrători le îndeplinesc în prezent. Așa cum arătam, lucrătorii cu cel mai mare risc de automatizare ajung în șomaj.*”

Studiul concluzionează următoarele:

1. **Lucrătorii cu risc mic** de pierdere a locului de muncă datorită digitalizării și automatizării, cei cu locuri de muncă ”sigure”, **se pot îndrepta**, cel mai probabil, **către tipul de antreprenoriat clasic orientat pe producție și creștere**, încorporat cu personalitate juridică;
2. **Lucrătorii cu risc mediu** de pierdere a locului de muncă datorită digitalizării și automatizării, cei cu aptitudini medii, **vor fi forțați să se îndrepte către tipul de antreprenoriat de ”necesitate”**, necorporalizat, fără personalitate juridică, **neavând astfel garantate în niciun fel veniturile și profitul necesare unui nivel de trai corect și sănătos** deoarece munca independentă este dovedită că nu este sustenabilă pe termen lung;
3. **Lucrătorii cu risc ridicat** de pierdere a locului de muncă datorită digitalizării și automatizării, cei cu aptitudini reduse sau cei necalificați, **nu se vor îndrepta către antreprenoriat, ci vor trebui să se ”specializeze” ajutați de politici publice sau să se adreseze direct mecanismelor de asistență socială, ceea ce va pune o presiune și mai mare asupra sistemului social.**

Este evident că avansul digitalizării, automatizării și conectivității va favoriza tot categoria care are apetitul și aptitudinile antreprenoriale mari, împreună cu riscul ocupațional cel mai mic de pierdere a locului de muncă datorat avansului tehnologic.

Argumentele care susțin că avansul tehnologic însuși va genera locuri de muncă nu au și fundamentarea socială necesară.

S-a demonstrat că nu se manifestă în realitate schimbări bruște ale apetitului antreprenorial, inclusiv pentru a ”beneficia” de avansurile tehnologice, acest apetit antreprenorial aparținând în continuare de o categorie socială deja existentă, deși cantitativ cea mai redusă numeric și care se confruntă cu cele mai reduse riscuri asociate dezvoltării tehnologice.

Dacă argumentele care susțin că avansul tehnologic, ne referim aici Digitalizarea Europei, „*societate europeană a gigabiților*” însuși va genera locuri de muncă se referă la **apariția forțată și creșterea numerică a tipul de antreprenoriat de ”necesitate”**, ca urmare a pierderii locurilor de muncă, **trebuie avută în vedere și latura calitativă unde există riscul cel mai mare din punct de vedere social**.

- **Calitatea conexiunii/performanțele de conectivitate NU SUNT FACTORII DETERMINANTI/EXCLUSIVI** pentru prosperitatea/**îmbunătățirea vieții comunităților.** între viteza conexiunii la internet și ceilalți parametrii socio-economici introduși în justificarea agenției Comisiei Europene nefiind în realitate o corelație.

Mai exact, România în 2018 are o poziție foarte bună (locul 5 mondial) la Calitatea conexiunilor la Internet, dar o poziție slabă la Prosperitate (45 mondial) și una și mai slabă la Calitatea Economică (60 mondial) în timp ce Islanda avea o poziție slabă (34 mondial) la Calitatea conexiunilor la Internet, dar o poziție bună la Prosperitate (11 mondial) și una excelentă la Calitatea Economică (1) iar Germania are o poziție medie (25 mondial) la Calitatea conexiunilor la Internet și o poziție bună la Prosperitate (14 mondial) și o poziție buna Calitatea Economică (11 mondial) exemplele pot continua cu Marea Britanie, Irlanda, Australia, Canada

Parametrii constituenți ai prosperității nu se limitează doar la aspectul economic ci și la alți parametri precum: mediul de afaceri, guvernanta, educația, sănătatea, siguranța, libertate personală, capital social, mediu natural.

Pentru a vă edifica, România ocupă la nivel mondial următoarele locuri la acești indicatori pe care Guvernul și membrii GLI 5G nu-i iau în considerare referindu-se la aceasta strategie:

- Calitatea economică: locul 60;
- Mediul de afaceri: locul 39;
- Guvernanța: locul 60;
- Educația: locul 39;
- Sănătatea: locul 81;
- Siguranța: locul 37;
- Libertate personală: locul 59;
- Capital social: locul 83;
- Mediu natural: locul 51.

Sursa: https://www.prosperity.com/globe/românia.

Așadar, România cu o viteză de top a conexiunii la internet, nu a performat la capitolele pe care emitenții acestei strategii le invocă în aceasta motivare. Textele de fundamentare de la impactul macroeconomic și impactul asupra mediului de afaceri sunt doar cuvinte fără conținut, parcă scoase dintr-o broșură de marketing a prestatorului de servicii telecom.

În fapt, implementarea forțată a tehnologie 5G prin această Strategie europeană pentru 5G aduce argumente care se contrazic, pe deoparte spun că este pentru acoperire în zone unde alte tehnologii nu ajung, iar pe de altă parte susțin că aceste tehnologii vor fi în zonele urbane acolo unde este cerere și infrastructură permisivă.

Prin această implementare abuzivă și nejustificată se promovează agresiv și vânzarea unei cantități imense suplimentare de spectru pentru 5G sub pretextul creșterii acoperirii serviciilor telecom în zonele izolate/retrase/rurale, zone care nu au fost încă acoperite cu 2G, 3G, 4G de corporațiile telecom, din motive evidente de lipsă a nevoii sau a capacității populației de cumpărare a serviciilor telecom, mai concret sărăcia. România, alături de Bulgaria are cei mai săraci dintre săracii Europei!

Sursa: https://monitorsocial.ro/indicator/saracii-români-sunt-cei-mai-saraci-dintre-saracii-europei/.

Mai mult, dependența tehnologiei 5G de frecvențe noi pentru acoperire extinsă (de ex. 700 MHz), transferă această dependență și la nivelul terminalelor client, permițând conectivitatea pe ”acoperirea extinsă” doar terminalelor compatibile cu respectiva frecvență. Ținem să menționăm că aceste terminale ”compatibile 5G” sunt în primul rând mult mai noi și rare, dar și mult peste puterea de cumpărare a zonelor rurale necesare a fi ”acoperite”. De aceea, acoperirea extinsă trebuie realizată pe serviciile actuale 2G, 3G sau 4G, pe benzile de frecvență similare (de ex. 800 sau 900 MHz) din spectrul existent/licențiat operatorilor.

Sursa: https://ec.europa.eu/digital-single-market/en/desi; https://ec.europa.eu/digital-single-market/en/scoreboard/românia.

SECURITATEA CIBERNETICĂ

World Global Research Report cotează securitatea cibernetică drept cel de-al treilea risc global în 2018, depășit numai de dezastrele naturale și catastrofele climatice.

“*Din informaţiile pe care le colectăm şi analizăm pot spune că în 2019 a crescut semnificativ numărul incidentelor de securitate, cu impact semnificativ, raportate către noi, cu peste 40%, de la 550 la aproape 800. Trecerea către 5G impune o funcţionare optimă a întregii reţele de acces. Dacă în 2017-2018* ***cele mai afectate servicii au fost cele de telefonie mobilă şi de mesagerie, anul trecut cele mai afectate au fost cele de internet mobil şi transmisiuni de***

***date mobile*, cu peste 10 milioane de conexiuni afectate.** *Iar numărul de incidente care au afectat principale categorii de resurse a fost în creştere faţă de anul 2018.*" VP ANCOM Eduard Lovin

Sursa: https://www.zf.ro/business-hi-tech/cand-va-trece-romania-la-5g-ce-spun-autoritatile-19163626

Odată cu apariția **IoT** (internetul lucrurilor) și a miliardelor de noi mașini conectate la Internet, senzori, obiecte, roboți, dispozitive etc. – toate facilitate și bazate pe 5G – atacurile cibernetice au devenit inevitabile. În plus, un sistem wireless este mult mai vulnerabil la asemenea atacuri decât un sistem cablat.

Vulnerabilități de securitate cibernetica în arhitectura 5G sunt uriașe iar paradigma, instrumentele și măsurile înaintate de Comisia Europeană către statele membre nu acoperă și nici nu pot acoperi masivul risc la care suntem expuși pentru niște ambiții doar de natura economica. Aceasta tehnologie este încă nestandardizată, neomologată și în curs de testare. Chiar și din punct de vedere economic, prioritățile României sunt: infrastructura rutieră, spitalele, modernizarea școlilor, locuri de muncă - inclusiv pentru milioanele de români plecați din țară etc..

Vulnerabilități de securitate în arhitectura 5G

În principiu, implementarea 5G se presupune că va genera beneficii uriașe de performanță și diversitate de aplicații prin utilizarea în arhitectura 5G a unor concepte și tehnologii complet noi față de generațiile anterioare, precum **MEC** (*Multi-Access Edge Computing*) și *Network Function Virtualization* (**NFV**), precum și alte tehnologii emergente. Aceste modificări sunt promovate ca fiind necesare în principal performanței și vitezei. În realitate, ele sunt necesare și operatorilor de telecomunicații pentru reducerea costurilor interne cu „tehnologia telecom", apărând noi riscuri de securitate și fronturi suplimentare de atac, existente în arhitectura rețelelor 5G.

De exemplu, conceptul **MEC** amintit mai sus **aduce cu sine vulnerabilități mari de securitate a datelor**. În termeni tehnici se spune ca *"**MEC** este o evoluție din zona cloud computing care aduce aplicațiile din zona centrelor de date centralizate către marginea rețelei și, prin urmare, mai aproape de utilizatorii finali și dispozitivele lor. Acest lucru creează, în esență, o scurtătură în livrarea de date/conținut între utilizator și rețeaua telecom, scurtând calea lungă de rețea care le-a 'separat'. **MEC**, prin caracteristicile principale care includ latența scăzută, lățimea mare de bandă și accesul în timp real la informațiile **RAN** (Radio Access Network) e o componenta cu o contribuție majoră la eficiența și viteza promovate de 5G, prin care se distinge arhitectura celei de-a 5-a generații de cele anterioare."*

Sursa: https://www.viavisolutions.com/en-us/5g-architecture.

Trebuie menționat că, din punct de vedere al securității datelor, centrele de date (care efectiv găzduiesc date și aplicații/servicii cloud) sunt, arhitectural, mult mai securizate decât poate fi **MEC**, cel puțin din punct de vedere al securității fizice, dar în special datorită existenței în proximitatea lor, pentru intervenție rapidă, a resurselor umane ce îndeplinesc atribuții în **SOC** (*Security Operations Center*). În cazul componentelor **MEC**, acestea nu pot fi monitorizate și intervenția asupra lor se poate face numai de la mare distantă, acestea fiind fizic instalate la nivelul stațiilor de acces radio (stâlpi și antene telecom).

Similar, în termeni tehnici se spune despre **NFV** ca: *"Virtualizarea funcțiilor de rețea (**NFV**) [...] [înlocuiește] diferite funcții de rețea, cum ar fi firewall-uri, echilibratoare de sarcina (load balancers) și routere cu instanțe virtualizate care rulează doar ca software, indiferent de hardware-ul pe care rulează. Acest lucru elimină necesitatea de a investi în multe elemente hardware costisitoare și poate accelera și timpul de instalare, oferind astfel mai rapid serviciile care generează venituri." Sursa: https://www.viavisolutions.com/en-us/5g-architecture*.

Înlocuirea doar cu software a unor echipamente special proiectate, testate și dedicate rulării unor funcții specifice și importante ale rețelei telecom, în special cele ce țin de **securitatea si accesul datelor**, reprezintă o **vulnerabilitate majora** ce ține de însăși arhitectura rețelelor 5G. Este de notorietate în industria IT că software-ul proiectat să fie portabil și independent de hardware (similar tehnologiei și serviciilor cloud) are, într-adevăr, o arhitectura mai „liberă" și mai „integrabilă" dar care, în realitate, **introduce și multiple vulnerabilități de securitate**. Aceste vulnerabilități provin, dacă nu întotdeauna de la codul software-ului în sine, cel puțin de la multiplele interfețe de integrare „liberă" care sunt expuse la exteriorul său. Acest tip de vulnerabilități nu există decât în foarte mică măsură în cazul echipamentelor hardware care îndeplinesc un scop sau o funcție precisă, cum ar fi securizarea traficului de rețea.

Pe măsură ce implementarea 5G continuă și componentele critice devin din ce în ce mai decuplate și virtualizate, operatorii vor trebui să monitorizeze și să evalueze continuu securitatea rețelei.

"Din punctul de vedere al CERT-RO, multitudinea de echipamente care vor invada spațiul nostru odată cu apariția tehnologiei 5G, faptul că vom vedea concret ce înseamnă noțiunea de smart, atât la nivel de orașe, transporturi, dar și personal, **evident că toate acestea vor aduce vulnerabilități**." CERT-RO - Cătălin Petrică Aramă.

Sursa: https://youtu.be/3tVq0f47sTk.

Vulnerabilități de securitate a protocoalelor 5G

„Actori cibernetici cu motivație strategică sau financiară pot beneficia de ușurința **compromiterii unor dispozitive IoT**, dar și de nivelul de inter-conectivitate a acestora în vederea accesării unei rețele. Acest aspect poate facilita crearea și dezvoltarea unor rețele de

boți utilizate în **derularea unor atacuri cibernetice** special concepute pentru a afecta disponibilitatea unor infrastructuri IT&C.

În anul 2019, cea de-a 5-a generație de viteză de transfer în mediul Internet pe telefonia mobilă se va extinde la nivel mondial, determinând creșterea vitezei de download de 6 ori, existând riscul de **creștere a numărului de atacuri de tip DDoS**, întrucât 5G va permite interconectarea unei largi game de dispozitive."

Sursa: https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2019.pdf.

Cercetătorii au descoperit o vulnerabilitate a protocoalelor de autentificare în rețea înainte ca implementările 5G să fie lansate. Într-o lucrare din 2019 care detaliază amenințările de confidențialitate pentru 3G, 4G și 5G, cercetătorii de la Universitatea Tehnică din Berlin, ETH Zurich și SINTEF Digital Norway au descoperit o vulnerabilitate care afectează protocolul **AKA** (*Authentication and Key Agreement*), utilizat ori de cate ori telefonul comunică cu rețelele mobile.

Sursa: https://eprint.iacr.org/2018/1175.pdf.

Noua vulnerabilitate permite potențialilor hoți de date să fure informații, cum ar fi numărul de apeluri și numărul de mesaje text trimise, **doar prin intermediul undelor radio 5G**, fără a accesa în vreun fel telefonul utilizatorului.

Sursa: https://www.zdnet.com/article/new-security-flaw-impacts-5g-4g-and-3g-telephony-protocols/.

Cercetătorii de la Universitatea Purdue și Universitatea din Iowa au prezentat **unsprezece noi probleme de proiectare în protocoalele 5G**, printre care faptul că ar putea să expună locația utilizatorului, să downgradeze serviciul 5G la 4G sau 3G, să extragă datele de pe telefon sau chiar să te urmărească atunci când efectuezi apeluri, text sau doar navighezi pe web.

"Lucrul care mă îngrijorează cel mai mult este că atacatorii pot ști locația utilizatorului." - Syed Rafiul Hussain, Purdue University.

Sursa: https://www.wired.com/story/5g-vulnerabilities-downgrade-attacks/.

Aceste riscuri si vulnerabilitati semnalate de specialistii in securitate cibernetica ce implica utilizatorilor finali 5G nu sunt acoperite corespunzător de instrumentele propuse de Comisia Europeană

Risc 6: Exploatarea rețelelor 5G de către criminalitatea organizată sau de către grupurile infracționale organizate care vizează utilizatorii finali

Risc R9: Exploatarea internetului obiectelor

Referința și mărturia la aceste riscuri este însăși propria sinteză a planurilor și propria evaluare a eficacității așteptate prezentate de Comisia de Comunicații la pagina 15 a setului de instrumente care stau la baza comunicării Comisiei Europene la adresa https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

Comisia de Comunicații prezintă aceste planuri de măsuri destinate celor 9 clase riscuri cibernetice ca fiind răspunsul la avalanșa de vulnerabilități cibernetice, cartografiate de altfel în Raportul ENISA, vulnerabilități care nu se limitează doar la nivelul operatorilor, cu foarte multe vulnerabilități se confruntă și **utilizatorul final**, noi **cetățenii**.

Se poate observa din tabelul prezentat la audieri și care se găsește în pagina următoare (***Table 3: simplified overview of measures in risk mitigation plans*** *(for more details, see annex 1, table 2,* pag.15) al setului de măsuri ca pentru **R9 - exploatarea IoT** (ultima coloană) sunt **doar 4 măsuri** planificate, mai mult acele 4 măsurile destinate acestei categorii de riscuri prezintă o **eficacitate medie și submedie**.

Măsurile de întâmpinarea ale riscurilor din categoriile R6 si R9 sunt predominant măsuri cu caracter birocratic de control, raportare, auditare pentru securitatea operatorului, **nu a utilizatorului final.** Preocuparea pentru SOC și NOC se referă la instrumente destinate rețelei 5G a operatorilor, nu la echipamentul 5G client, din mâna noastră, casa noastră, computerul nostru etc.

De asemenea se poate observa din tabelul prezentat că accentul se pune foarte mult pe puterea **autoritățile de reglementare naționale și pe operatori**, acestora fiindu-le dedicate cele mai multe măsuri și facilități, în timp ce instrumentele, măsurile destinate cetățenilor utilizatori sunt cu mult mai puține și mai puțin eficiente în fața amenințărilor cibernetice survenite în urma implementării acestei tehnologii invazive, disruptive 5G.

În opinia noastră, noi utilizatorii finali suntem lăsați fără apărare în fața **multiplelor, sofisticatelor și din ce în ce mai agresivelor atacuri cibernetice** venite o dată cu tehnologia mobilă 5G, pe banii noștri, pe viața și proprietatea noastră privată, pe drepturile noastre fundamentale. Pe lângă multitudinea de fonduri financiare destinate industriei comunicațiilor pentru “inovare, cercetare si implementare 5G”, se cristalizează încă o dovadă că implementarea tehnologiei 5G are un proeminent caracter și interes economic, tehnologic, în detrimentul interesului social, al bunăstării cetățeanului.

Table 3: simplified overview of measures in risk mitigation plans *(for more details, see annex 1, table 2)*

MEASURES	Indicative implementation timeframe			Potential implementation factors				SPECIFIC MEASURES	RISKS									
	Short-term	Medium-term	Long-term	Resource costs	Sector specific economic impact	Sector specific economic impact	Broader economic / societal impact		R1: Misconfiguration of networks	R2: Lack of access controls	R3: Low product quality	R4: Dependency on a single supplier	R5: State interference through 5G supply chain	R6: Exploitation of 5G networks by org. crime	R7: Significant disruption of crit. Infras. services	R8: Massive failure due to power interruption	R9: IoT exploitation
a) Regulatory powers	✓			✓	✓	✓	✓	SM 01									
								SM 02									
b) Third party suppliers	✓			✓	✓	✓	✓	SM 03									
								SM 04									
c) Diversification of suppliers	✓	✓		✓	✓	✓	✓	SM 05									
								SM 06									
d) Sustainability and diversity of 5G supply and value chain	✓	✓	✓	✓	✓	✓	✓	SM 07									
								SM 08									
a) Network security – baseline measures	✓			✓	✓			TM 01									
								TM 02									
b) Network security – 5G specific measures	✓			✓	✓			TM 03									
								TM 04									
								TM 05									
								TM 06									
								TM 07									
c) Requirements related to suppliers' processes and equipment		✓	✓	✓	✓	✓		TM 08									
								TM 09									
								TM 10									
d) Resilience and continuity	✓			✓	✓			TM 11									

Expected effectiveness:

Very low — Very high

SIGURANȚA MEDIULUI ÎNCONJURĂTOR

Comisia nu prezintă instrumente și măsuri care să reducă amprenta energetică a infrastructurii rețelelor 5G și care să promoveze reciclarea reziduurilor electronice în contextul impunerii implementării sale actuale, rapide și nelimitate. Comisia nu prezinta interes și preocupări în promova măsuri, a aloca fonduri financiare pentru studiul impactului implementării acestei tehnologii asupra mediului și a ecosistemelor asociate, în Europa și la nivel mondial.

Nu sunt luate în considerare și următoarele aspecte:

- Energia enorma, consumată de toate aceste obiecte interconectate, "internet al tuturor lucrurilor"– echipamente de rețea, mașini, aplicații, senzori, camere video de supraveghere etc.;

- Cantitatea astronomică de energie care este necesară pentru a crea toate aceste "lucruri" care aparțin de **IoT**, instrumente și infrastructură asociată (energie încorporată);
- Cantitatea de dioxid de carbon (CO2) eliberată în atmosferă de producerea energiei necesare (generate în bună parte de combustibili fosili) folosite de sursele wireless în continuă creștere;
- Cantitatea enormă de energie necesară pentru a asigura funcționarea punctelor de centralizare/tranzitare a datelor (antene, servere, routere, internoduri);
- Energia suplimentară necesară pentru a transporta datele wireless prin intermediul aerului, în loc de folosirea energetic eficientă a fibrei optice sau cablurilor.

Odată cu implementarea tehnologiei 5G și a Internetului Lucrurilor (IoT), echipamentele noi ale rețelei 5G de ordinul miliardelor, împreuna cu obiectele casnice (mașini de spălat, fierbătoare, frigidere etc.) se vor adăuga categoriei de reziduuri electronice - *e-waste*. În acest context, implementarea tehnologiei 5G prin generarea de cantități masive de deșeuri este în contradicție flagrantă cu principiile economiei moderne a secolului XXI, anume economia circulară, bazată pe conceptul *zero waste*.

Concluzie

Tehnologia 5G este creată mai mult pentru mașini și obiecte decât pentru sănătatea oamenilor. În mod ironic, tot oamenii sunt cei care plătesc și vor plăti toate costurile aduse de acest fals și toxic "progres", care nu numai că nu le este destinat, dar le afectează ireversibil bunăstarea, sănătatea și viața. Noi, cetățenii Europei, și urmașii noștri vom fi cei care plătim - cu bani, cu sănătate, cu libertate, cu echilibrul mediului natural, cu drepturi fundamentale, cu

suveranitate - această ambiție pentru profit și control a anumitor entități economice și grupuri de interese, numită 5G.

Coaliția STOP 5G România

Coaliția STOP 5G România este o mișcare civică fără formă juridică cu o susținere largă a cetățenilor României:

- **28 566 semnatari** ai Petiției „Cerem interzicerea implementării și dezvoltării rețelei 5G în România";
- **17 659 semnatari** ai Petiției „Cerem Ministerului Sănătății să evalueze implementarea tehnologiei 5G în România";
- **81 de organizații** semnatare a Memoriul național STOP 5G în România.

Misiunea Coaliției STOP 5G este de a **proteja drepturile constituționale ale cetățenilor României**, printre care: dreptul la viață, dreptul la sănătate, dreptul la un mediu curat, dreptul la proprietate, dreptul la intimitate etc. Facem aceasta inclusiv prin stoparea demersurilor Guvernului României și ale ANCOM legate de implementarea tehnologiilor 5G în România și oprirea oricărui demers legislativ referitor la aceste tehnologii invazive, nesustenabile, experimentale și dăunătoare întregului ecosistem.

Coaliția STOP 5G are ca scop responsabilizarea tuturor actorilor sociali și politici pentru angajarea răspunderii Instituțiilor Statului, a funcționarilor și a tuturor factorilor de decizie în raport cu necesitatea de a respecta drepturile constituționale prin respectarea și aplicarea **principiului precauției** care **protejează viața, sănătatea oamenilor precum și a mediului natural**.

Date de contact: website: stop5GRomania.ro email: contact@stop5gromania.ro

Membru fondator: Asociația Pro Consumatori România
Președinte Costel Stanciu, tel: 0723 004 407, e-mail: office@apc-romania.ro.

Reprezentanții societății civice care au contribuit la întocmirea documentației pentru **Comisia pentru afaceri europene din Senat**:

Pompiliu Diplan - *Alianța Părinților din România;*
Mădălina Apostol - *Centrul de Cercetare și Dezvoltare AXIO*;
Adrian Aciu - *Asociația Pro Vita*;
Costel Stanciu - *Asociația Pro Consumatori*;
Luminița Simoiu - *Asociația Civică Pentru Viață;*
Eugen Lucan - *Asociația Angel;*
George Stoian - *Asociația Pro Decizii Informate.*

Data: 27.05.2020