

Germania și Austria: Precursorii masurilor de securitate 5G?



Subiectul securității cibernetice a rețelelor 5G se afla, în prezent, pe masa discuțiilor în toate statele europene. Etapele preliminare pentru implementarea masurilor de securitate a rețelelor 5G ar fi trebuit parcurse până la data de 30 aprilie, potrivit calendarului propus inițial de către Comisia Europeană¹. Ulterior, urma să fie realizat un raport comun cu privire la implementarea acestor măsuri în fiecare stat.

Având în vedere că securitatea cibernetică este tratată ca parte a securității naționale, iar potrivit art. 4 alin. (2) din Tratatul privind Uniunea Europeană² „securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat”, prin regulile propuse în EU Toolbox se urmărește coordonarea măsurilor implementate la nivel național în Uniunea Europeană³. Reamintim că acest document elaborat de grupul de Cooperare NIS propune atât *masuri strategice*, cât și *masuri tehnice* pentru limitarea riscurilor de securitate cibernetică.

În privința măsurilor strategice, în EU Toolbox se menționează că în unele state au fost implementate deja, iar altele pregătesc o legislație similară, context în care coordonarea între statele membre sau coordonarea la nivelul Uniunii Europene ar fi benefică⁴.

Ne propunem în continuare să facem o analiză succintă a măsurilor în curs de implementare sau deja implementate prin diverse acte normative în alte țări europene, având în vedere faptul că este de așteptat ca România să urmeze exemplul altor țări în procesul de aliniere la cerințele cuprinse în EU Toolbox.

În ceea ce privește România, în data de 21 mai 2020, a fost constituit un grup de lucru interinstituțional pentru elaborarea unui raport privind punerea în aplicare a măsurilor-cheie identificate din setul de instrumente al UE pentru atenuarea eficace a riscurilor și asigurarea securității rețelelor 5G⁵. Acest grup de lucru nu a făcut, încă, publice lucrările sale în acest domeniu.

Însă, la nivelul Uniunii Europene, state precum Germania și Austria au propus deja instrumente de implementare a acestor măsuri în legislația internă pentru atenuarea eficace a riscurilor și asigurarea securității rețelelor 5G.

Astfel, Agenția Federală a Rețelelor de Electricitate, Gaz, Telecomunicații, Poșta și Transport Feroviar din Germania a supus dezbaterii publice „Catalogul cerințelor de securitate pentru operarea sistemelor de telecomunicații și procesare a datelor cât și pentru prelucrarea datelor personale”⁶ („Catalogul Cerințelor de Securitate din Germania”), care, de asemenea, acordă un rol important operatorilor de comunicații în asigurarea securității rețelelor.

Principalele prevederi ale Catalogului Cerințelor de Securitate din Germania impun operatorilor să adopte:

- a. masuri de securitate cu privire la angajați;
- b. masuri pentru securitatea fizica a echipamentelor și a rețelelor (fiind prevazute expres masuri cu privire la controlul accesului și a intrării în sistemele de rețea și informații);
- c. masuri de comunicare și de raportare a incidentelor de securitate;
- d. proceduri de monitorizare și testare, inclusiv simulări pentru situații de urgență;
- e. masuri de securitate pentru protejarea datelor cu caracter personal.
- f. masuri pentru garantarea integrității și disponibilității sistemelor de rețea și informații;

În plus, Catalogul Cerințelor de Securitate din Germania, stabilește în sarcina operatorilor obligații cu privire la:

- a. folosirea componentelor critice certificate;
- b. monitorizarea securității;
- c. respectarea principiului neutralității internetului;
- d. mecanisme criptografice și de management al cheilor;
- e. certificarea componentelor pentru realizarea funcțiilor critice;
- f. certificarea credibilității producătorilor și a furnizorilor.

Interesant este modul în care Germania a prevazut verificarea celei din urma cerințe, privind certificarea credibilității producătorilor și a furnizorilor. Normele germane prevad ca pentru verificarea credibilității producătorului, furnizorii vor completa o declarație de încredere al carei conținut minim este stabilit de actul normativ menționat mai sus, dar, care poate fi completat cu anumite criterii de catre operatori.

Totodata, Catalogul Cerințelor de Securitate din Germania mai identifica o alta posibila metoda de verificare a operatorilor și furnizorilor, lasând Agenției Federale a Rețelelor de Electricitate, Gaz, Telecomunicații, Poșta și Transport Feroviar posibilitatea de a dispune ca aceștia sa fie supuși unui audit realizat de un organism independent calificat sau de o autoritate naționala competenta, potrivit dispozițiilor art. 109 alin. (7) din TKG⁷.

Și în Austria a fost supus dezbaterii publice, în data de 24 aprilie 2020, de catre Autoritatea de Reglementare în Domeniul Telecomunicațiilor - Rundfunk und Telekom Regulierungs-GmbH (RTR) – („**Autoritatea de Reglementare**”) proiectul ordonanței referitoare la obligațiile minime de securitate a operatorilor de rețele de comunicații electronice⁸.

Proiectul de ordonanța propus în Austria instituie în sarcina operatorilor (a) un set comun de reguli aplicabile tuturor rețelelor de telecomunicații și (b) obligații particulare pentru protejarea securității rețelelor 5G.

Astfel, printre regulile stabilite în sarcina operatorilor, regasim:

- a. obligația de a notifica un incident de securitate care are un impact semnificativ asupra securității rețelei de comunicații;
- b. obligația de a concepe și de a implementa o politica de securitate care sa asigure un nivel adecvat de securitate în

raport cu riscurile existente;

c. o serie de obligații pentru operatorii de rețele 5G cu mai mult de 100.000 de utilizatori, cum ar fi:

- sa depuna un raport de audit în mod regulat;
- sa depuna o declarație de conformitate care sa ateste respectarea unor standarde internaționale precum 3GPP, expres menționate în anexa acestui ordin;
- sa asigure funcționarea centrului de operațiuni de rețea și a centrului de operațiuni de securitate în Uniunea Europeana;
- sa monitorizeze efectiv toate componentele critice și părțile sensibile ale rețelelor 5G prin centrul de operațiuni de rețea și prin centrul de operațiuni de securitate;
- sa previna schimbarea neautorizată a rețelelor sau a componentelor;
- sa asigure protecția fizică a componentelor critice și sensibile ale rețelelor 5G;
- sa restrângă accesul la personalul competent și calificat, supus anterior unor verificări de securitate;
- sa folosească instrumente adecvate sa asigure integritatea software când sunt operate actualizări software;
- sa stabilească o strategie care sa asigure furnizarea infrastructurii de către mai mulți furnizori, inclusiv prin luarea în considerare a constrângerilor tehnice și a cerințelor de interoperabilitate în diferite părți ale rețelelor 5G.

Asemenea măsurilor de securitate impuse operatorilor de date cu caracter personal⁹ și a celor prevăzute de Codul European al Comunicațiilor Electronice¹⁰, Autoritatea de Reglementare din Austria subliniază faptul ca trebuie avut în vedere de către operatori „standardul stadiului actual al tehnologiei” („*state of the art*”), astfel ca, politica de securitate informațională va cuprinde cel puțin:

- măsuri de management al riscului;
- măsuri de securitate cu privire la angajați;
- măsuri de securitate fizice;
- monitorizare, auditare și testare.

Din punctul de vedere al Autorității de Reglementare din Austria, pentru implementarea unui mecanism de evaluare a furnizorilor în raport de criteriile menționate în setul de măsuri pentru reducerea riscurilor de securitate a rețelelor 5G, este necesar un alt temei legal, respectiv, adoptarea unui alt act normativ de către autoritățile competente. Cu privire la strategia de asigurare a mai multor furnizori, proiectul de ordonanță din Austria menționează evitarea sau limitarea dependenței față de un furnizor considerat riscant.

Măsurile descrise mai sus, adoptate sau în curs de adoptare în cele două țări europene au ca scop stabilirea de criterii transparente și obiective pentru verificarea participanților la piața echipamentelor 5G.

Într-un alt material pe care l-am publicat am prezentat rezerve cu privire la compatibilitatea unor măsuri de excludere sau de limitare a accesului unor competitori pe piața din perspectiva obligațiilor internaționale asumate de către Uniunea Europeană și de către statele membre¹¹.

Între timp, în spațiul public s-a exprimat și opinia ca măsurile de limitare sau restrângere a furnizorilor de echipamente par a încălca principiile enunțate de legislația europeană și națională în domeniul telecomunicațiilor, respectiv principiile obiectivității, transparenței, proporționalității și al nediscriminării.¹²

Cele două acte normative propuse în Austria și Germania dovedesc, însă, ca EU Toolbox poate fi implementat asigurându-se, totodată, și menținerea concurenței pe piața produselor și serviciilor pentru construirea și întreținerea rețelelor 5G, precum și respectarea principiilor mai sus enumerate.

Astfel, pe de-o parte, sunt constituite măsuri de prevenire a accesului neautorizat la rețele, iar pe de alta parte, sunt instituite și reguli de certificare obiectivă a echipamentelor ce ar urma să fie încorporate în rețeaua de telecomunicații, pârghii prin care să poată fi realizată o evaluare continuă de către operatori sau autorități a securității rețelelor de telecomunicații.

În concluzie, implementarea măsurilor de securitate cibernetică rămâne o chestiune de competență a statelor membre. Însă, pentru asigurarea unei implementări coordonate și a asigurării unor condiții similare de implementare a tehnologiei 5G la nivelul Uniunii Europene, menite să asigure predictibilitate, precum și pentru evitarea fragmentării piețelor, ar fi preferabil ca actele normative adoptate de statele membre să conțină măsuri similare celor deja adoptate sau aduse la cunoștința publicului, spre consultare.

De altfel, necesitatea evitării fragmentării piețelor prin instituirea unor bariere administrative restrictive a fost subliniată și de către Thierry Breton, Comisarul European pentru Piața Internă, care a declarat într-un comunicat recent ca: „*Rețelele wireless 5G reprezintă un pilon al dezvoltării socioeconomice a Europei, deoarece vor permite furnizarea de noi servicii în sectorul sănătății și al îngrijirilor medicale, al energiei, al transporturilor, al educației și în multe alte domenii. Importanța acestora este și mai evidentă în momentul de față, întrucât rețelele vor juca un rol esențial în redresarea noastră în urma crizei provocate de coronavirus. Împreună cu statele membre, trebuie să deschidem calea pentru introducerea la timp a tehnologiei 5G, fără bariere administrative restrictive, lucru care va aduce cu sine o cerere semnificativă din partea industriei noastre și va amplifica inovarea și competitivitatea la nivel european*”¹³.

1. Disponibil la https://ec.europa.eu/commission/presscorner/detail/en/IP_20_123 (consultat în data de 02.07.2020).

2. Disponibil la https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0001.02/DOC_1&format=PDF (consultat în data de 02.07.2020)

3. A se vedea secțiunea 2 din EU Toolbox – „*Obiectivele EU Toolbox sunt reprezentate de identificarea posibilelor măsuri comune care ar putea diminua principalele riscuri de securitate cibernetică a rețelelor 5G, astfel cum acestea au fost identificate în raportul de risc efectuat la nivelul Uniunii Europene și să asigure îndurmare în ceea ce privește selectarea măsurilor care ar trebui prioritizate în planurile de prevenire și minimizare a riscurilor la nivel național și la nivelul Uniunii. Se procedează în această manieră pentru a fi creat un cadru robust de măsuri care să asigure un nivel adecvat de securitate al rețelelor 5G în Uniunea Europeană și pentru a coordona abordările membrilor Uniunii Europene.*” (traducerea noastră).

4. A se vedea secțiunea 5.1. din EU Toolbox: „*Implementarea măsurilor strategice poate presupune legislație specifică la nivel național pentru asigurarea deplină a impactului măsurii. Unele State Membre au implementat deja legislație referitoare la măsurile strategice și altele pregătesc legislație similară. În viitor, cooperarea între Statele Membre sau la nivelul Uniunii Europene ar putea fi benefică pentru a promova abordări convergente.*” (traducerea noastră).

5. "Memorandum pentru înființarea Grupului de lucru 5G pentru identificarea măsurilor strategice și tehnice cheie din setul de instrumente al UE pentru atenuarea eficace a riscurilor și asigurarea securității rețelelor 5G necesare a fi implementate de România, respectiv pentru elaborarea raportului privind punerea în aplicare a acestora la nivel național", disponibil la <https://sgg.gov.ro/new/wp-content/uploads/2020/05/MEMO-6.pdf> (consultat la data de 02.07.2020).

6. Disponibil la

https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/aktualisierung_sicherheitsanforderungen/aktualisierung_sicherheitsanforderungen-node.html;jsessionid=BA3A1C931ADD0B5FB15E3B85CE19A79E (consultat la data de 02.07.2020)

7. Telecommunications Act (Telekommunikationsgesetz, TKG)

8. Disponibil la https://www.rtr.at/de/inf/konsult_NSiV_2020 (consultat în data de 02.07.2020).

9. art. 25 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor): „Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate.”

10 art. 40 pct. 1 din Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice - Codul European al Comunicațiilor Electronice

11. Ion Dragne, Alexandru Dragne, Dragne & Asociații „Compatibilitatea măsurilor pentru siguranța cibernetică a sistemului 5G cu libertatea comerțului”, 2020, disponibil la <https://www.universuljuridic.ro/compatibilitatea-masurilor-pentru-siguranța-cibernetica-a-sistemului-5g-cu-libertatea-comertului/> (consultat la data de 02.07.2020)

12. Alina Popescu, Cristina Crețu, Maravela, Popescu și Asociații: „Provocări juridice în implementarea setului comun de instrumente 5G și posibile efecte prejudiciabile asupra furnizorilor de comunicații electronice și asupra consumatorilor”, 2020, disponibil la <https://financialintelligence.ro/maravela-popescu-si-asociații-provocări-juridice-in-implementarea-setului-comun-de-instrumente-5g-si-posibile-efecte-prejudiciabile-asupra-furnizorilor-de-comunicații-electronice-si-asupra-consumatorilor/> (consultat la data de 02.07.2020)

13. Declarație disponibilă la

<https://www.euractiv.ro/eu-elections-2019/noi-reguli-pentru-simplificarea-instalării-rețelelor-5g-in-ue-ce-s-a-discutat-in-senatul-romaniei-19745> (consultat la data de 02.07.2020).

