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 pâna la data de 30 aprilie, potrivit calendarului propus inițial de catre Comisia Europeana[1]. Ulterior, urma sa fie realizat un raport comun cu privire la implementarea acestor masuri în fiecare stat.

Având în vedere ca securitatea cibernetica este tratata ca parte a securității naționale, iar potrivit art. 4 alin. (2) din Tratatul privind Uniunea Europeana[2] „*securitatea națională ramâne responsabilitatea exclusiva a fiecarui stat*", prin regulile propuse in EU Toolbox se urmarește coordonarea masurilor implementate la nivel național în Uniunea Europeana[3]. Reamintim ca acest document elaborat de grupul de Cooperare NIS propune atât *masuri stategice*, cât și *masuri tehnice* pentru limitarea riscurilor de securitate cibernetica.

În privința masurilor strategice, în EU Toolbox se menționeaza ca în unele state au fost implementate deja, iar altele pregatesc o legislație similara, context în care coordonarea între statele membre sau coordonarea la nivelul Uniunii Europene ar fi benefica[4].

Ne propunem în continuare sa facem o analiza succinta a masurilor în curs de implementare sau deja implementate prin diverse acte normative în alte țari europene, având în vedere faptul ca este de așteptat ca România sa urmeze exemplul altor țari 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 masurilor-cheie identificate din setul de instrumente al UE pentru atenuarea eficace a riscurilor și asigurarea securității rețelelor 5G[5]. Acest grup de lucru nu a facut, înca, publice lucrarile sale în acest domeniu.

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

Astfel, Agenția Federala 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, acorda un rol important operatorilor de comunicații în asigurarea securității rețelelor.

Principalele prevederi ale Catalogului Cerințelor de Securitate din Germania impun operatorilor sa 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 intrarii în sistemele de rețea și informații);

c. masuri de comunicare și de raportare a incidentelor de securitate;

d. proceduri de monitorizare și testare, inclusiv simulari pentru situații de urgența;

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. ceritificarea componentelor pentru realizarea funcțiilor critice;

f. certificarea credibilității producatorilor și a furnizorilor.

Interesant este modul în care Germania a prevazut verificarea celei din urma cerințe, privind certificarea credibilității producatorilor și a furnizorilor. Normele germane prevad ca pentru verificarea credibilității producatorului, 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 națională competenta, potrivit dispozițiilor art. 109 alin. (7) din TKG[7].

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 electrionice[8].

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 securtității 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 operatiuni de retea 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 operatiuni de retea și prin centrul de operațiuni de securitate;
- sa previna schimbarea neautorizata a rețelelor sau a componentelor;
- sa asigure protecția fizica a componentelor critice și sensibile ale rețelelor 5G;
- sa restrânga accesul la personalul competent și calificat, supus anterior unor verificari de securitate;
- sa foloseasca instrumente adecvate sa asigure integritatea software când sunt operate actualizari software;
- sa stabileasca o stategie care sa asigure furnizarea infrastructurii de catre mai mulți furnizori, inclusiv prin luarea în considerare a constrângerilor tehnice și a cerințelor de interoperabilitate în diferite părți alte rețelelor 5G.

Asemenea masurilor de securitate impuse operatorilor de date cu caracter personal[9] și a celor prevazute de Codul European al Comunicațiilor Electronice[10], Autoritatea de Reglementare din Austria subliniaza faptul ca trebuie avut în vedere de catre operatori „standardul stadiului actual al tehnologiei" („*state of the art*"), astfel ca, politica de securitate informațională va cuprinde cel puțin:

- masuri de management al riscului;
- masuri de securitate cu privire la angajați;
- masuri 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 masuri pentru reducerea risicurilor de securitate a rețelelor 5G, este necesar un alt temei legal, respectiv, adoptarea unui alt act normativ de catre autoritățile competente. Cu privire la strategia de asigurare a mai multor furnizori, proiectul de ordonanța din Austria menționeaza evitarea sau limitarea dependenței fața de un furnizor considerat riscant.

Masurile descrise mai sus, adoptate sau în curs de adoptare în cele doua țari 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 masuri de excludere sau de limitare a accesului unor competitori pe piața din perspectiva obligațiilor internaționale asumate de catre Uniunea Europeana și de catre statele membre[11].

Între timp, în spaţiul public s-a exprimat şi opinia ca masurile de limitare sau restrângere a furnizorilor de echipamente par a încalca principiile enunţate de legislatia europeana şi naţionala în domeniul telecomunicaţiilor, respectiv principiile obiectivitaţii, transparenţei, proproţionalitaţii şi al nediscriminarii.[12]

Cele doua acte normative propuse în Austria şi Germania dovedesc, însa, ca EU Toolbox poate fi implementat asigurându-se, totodata, şi menţinerea concurenţei pe piaţa produselor şi serviciilor pentru construirea şi întreţinerea reţelelor 5G, precum şi respectarea principiilor mai sus enumerate.

Astfel, pe de-o parte, sunt constituite masuri de prevenire a accesului neutorizat la reţele, iar pe de alta parte, sunt instituite şi reguli de certificare obiectiva a echipamentelor ce ar urma sa fie încorporate în reţeaua de telecomunicaţii, pârghii prin care sa poata fi realizata o evaluare continua de catre operatori sau autoritaţi a securitaţii reţelelor de telecomunicaţii.

În concluzie, implementarea masurilor de securitate cibernetica ramâne o chestiune de competenţa a statelor membre. Însa, pentru asigurarea unei implementari coordonate şi a asigurarii unor condiţii similare de implementare a tehnologiei 5G la nivelul Uniunii Europene, menite sa asigure predictibilitate, precum şi pentru evitarea fragmentarii pieţelor, ar fi preferabil ca actele normative adoptate de statele membre sa conţina masuri similare celor deja adoptate sau aduse la cunoştinţa publicului, spre consultare.

De altfel, necesitatea evitarii fragmentarii pieţelor prin instituirea unor bariere administrative restrictive a fost subliniata şi de catre Thierry Breton, Comisarul European pentru Piata Interna, care a declarat într-un comunicat recent ca: „*Reţelele wireless 5G reprezinta un pilon al dezvoltarii socioeconomice a Europei, deoarece vor permite furnizarea de noi servicii în sectorul sanataţii şi al îngrijirilor medicale, al energiei, al transporturilor, al educaţiei şi în multe alte domenii. Importanţa acestora este şi mai evidenta în momentul de faţa, întrucât reţelele vor juca un rol esenţial în redresarea noastra în urma crizei provocate de coronavirus. Împreuna cu statele membre, trebuie sa deschidem calea pentru introducerea la timp a tehnologiei 5G, fara bariere administrative restrictive, lucru care va aduce cu sine o cerere semnificativa din partea industriei noastre şi va amplifica inovarea şi competitivitatea la nivel european*[13]”.

---

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

3. A se vedea secţiunea 2 din EU Toolbox – ”*Obiectivele EU Toolbox sunt reprezentate de identificarea posibilelor masuri comune care ar putea diminuna principalele riscuri de securitate cibernetica a reţelelor 5G, astfel cum acestea au fost identificate în raportul de risc efectuat la nivelul Uniunii Europene şi sa asigure îndurumare în ceea ce priveşte selectarea masurilor care ar trebui prioritizate în planurile de prevenire şi minizare a riscurilor la nivel naţional şi la nivelulul Uniunii. Se procedeaza în aceasta maniera pentru a fi creat un cadru robust de masuri care sa asigure un nivel adecvat de securitate al reţelelor 5G în Uniunea Europeana şi pentru a coordona abordarile membrilor Uniunii Europene*.” (traducerea noastra).

4. A se vedea secţiunea 5.1. din EU Toolbox: „*Implementarea masurilor strategice poate prespune legislaţie specifica la nivel naţional pentru asigurarea deplina a impactului masurii. Unele State Membre au implementat deja legislaţie referitoare la masurile strategice şi altele pregatesc legislaţie similara. În viitor, cooperarea între Statele Membre sau la nivelul Uniunii Europene ar putea fi benefica pentru a promova abordari convergente*.” (traducerea noastra).

5. "*Memorandum pentru înființarea Grupului de lucru 5G pentru identificarea masurilor 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 in 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 implementarii, si natura, domeniul de aplicare, contextul si scopurile prelucrarii, precum si riscurile cu grade diferite de probabilitate si gravitate pentru drepturile si libertatile persoanelor fizice pe care le prezinta prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât si în cel al prelucrarii în sine, pune în aplicare masuri tehnice si organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate sa puna în aplicare în mod eficient principiile de protectie a datelor, precum reducerea la minimum a datelor, si sa integreze garantiile necesare în cadrul prelucrarii, pentru a îndeplini cerintele prezentului regulament si 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 Electonice

11. Ion Dragne, Alexandru Dragne, Dragne & Asociatii „*Compatibilitatea masurilor pentru siguranța cibernetica a sistemului 5G cu libertatea comerțului*", 2020, disponibil la https://www.universuljuridic.ro/compatibilitatea-masurilor-pentru-siguranta-cibernetica-a-sistemului-5g-cu-libertatea-comertului/ (consultat la data de 02.07.2020)

12. Alina Popescu, Cristina Crețu, Maravela, Popescu si Asociatii: „*Provocari juridice în implementarea setului comun de instrumente 5G si posibile efecte prejudiciabile asupra furnizorilor de comunicatii electronice si asupra consumatorilor*", 2020, disponibil la https://financialintelligence.ro/maravela-popescu-si-asociatii-provocari-juridice-in-implementarea-setului-comun-de-instrumente-5g-si-posibile-efecte-prejudiciabile-asupra-furnizorilor-de-comunicatii-electronice-si-asupra-consumato/ (consultat la data de 02.07.2020)

13. Declarație disponibila la https://www.euractiv.ro/eu-elections-2019/noi-reguli-pentru-simplificarea-instalarii-retelelor-5g-in-ue-ce-s-a-discutat-in-senatul-romaniei-19745 (consultat la data de 02.07.2020).