RĂSPUNSURILE COMISIEI EUROPENE LA RAPORTUL SPECIAL AL CURȚII DE CONTURI EUROPENE: „IMPLEMENTAREA TEHNOLOGIEI 5G ÎN UE: ÎNTÂRZIERI ÎN INSTALAREA REȚELELOR ȘI PROBLEME DE SECURITATE ÎNCĂ NEREZOLVATE”

SINTEZĂ

Observațiile introductive ale Comisiei

I. Instalarea rapidă și sigură a rețelelor 5G reprezintă o prioritate majoră pentru Comisia Europeană. Protejarea rețelelor 5G împotriva amenințărilor cibernetice presupune evaluarea și atenuarea amenințărilor și riscurilor. Aceste amenințări și riscuri au fost identificate și evaluate în comun de statele membre, cu sprijinul Comisiei și al ENISA și, pornind de la această evaluare, au fost identificate o serie de măsuri cuprinzătoare pentru atenuarea riscurilor identificate. Deși în unele state membre lucrările sunt în curs, o mare parte a acestora au consolidat deja, pe baza setului de instrumente al UE, cerințele de securitate pentru rețelele 5G sau sunt în curs de consolidare a acestora.

Setul de instrumente al UE a fost recunoscut ca un cadru cuprinzător pentru abordarea riscurilor de securitate legate de tehnologia 5G.

Acțiunea coordonată privind securitatea cibernetică a rețelelor 5G la nivelul UE și setul de instrumente al UE se încadrează într-un cadru european mai larg pentru protecția rețelelor de comunicații electronice și a altor infrastructuri critice și completează măsurile existente, cum ar fi Codul european al comunicațiilor electronice, cadrul privind telecomunicațiile, Regulamentul privind securitatea cibernetică și Directiva privind securitatea rețelelor (Directiva NIS) și, după caz, normele privind libera circulație prevăzute în tratat și în Carta drepturilor fundamentale a UE.

III. Tehnologia 5G va juca un rol esențial în economia și societatea noastră digitală în anii următori. Trebuie să luăm măsuri pentru a garanta siguranța cibernetică a rețelelor 5G și pentru a asigura rezistența lor în fața amenințărilor și incidentelor cibernetice din ce în ce mai numeroase. Acesta este motivul pentru care Comisia și statele membre au instituit un proces de coordonare care vizează definirea și punerea în aplicare a unui cadru de securitate cuprinzător privind rețelele 5G, sub forma unui set de măsuri de reducere a riscurilor. convenit în ianuarie 2020, pentru a aborda în mod eficace și coordonat riscurile majore pentru rețelele 5G, cum ar fi intruziunea informatică infracțională, spionajul și sabotajul. Deși în unele state membre lucrările sunt în curs, o mare parte a acestora au consolidat deja, pe baza setului de instrumente al UE, cerințele de securitate pentru rețelele 5G sau sunt în curs de consolidare a acestora:

VII. Setul de instrumente al UE oferă un cadru pentru promovarea coerenței pe piața internă, cu respectarea concomitentă a competențelor naționale în materie de securitate în acest domeniu.

În ceea ce privește abordarea statelor membre față de furnizorii cu grad ridicat de risc, Comisia consideră că va fi posibil să se efectueze o evaluare concludentă numai atunci când vor fi disponibile mai multe informații.

Pe durata procesului de punere în aplicare, Comisia colaborează cu statele membre în cadrul Grupului de cooperare NIS cu scopul de a promova alinierea și convergența abordărilor naționale.

IX. (Prima liniuță) Comisia acceptă recomandarea.

A doua liniuță - Comisia acceptă recomandarea.

A treia liniuță - Comisia acceptă recomandarea.

Comisia va efectua evaluarea ținând seama de competențele naționale.

INTRODUCERE

04. Deși recunoaște existența riscurilor de securitate legate de tehnologia 5G, Comisia subliniază că această tehnologie și standardele aferente rețelelor 5G pot genera și îmbunătățiri în materie de securitate în comparație cu generațiile de rețele anterioare.

OBSERVAȚII

30. Deși tehnologia 4G acoperă deja o gamă largă de servicii, serviciile 5G ar trebui să reprezinte un adevărat „salt", o schimbare majoră în comparație cu tehnologia 4G, motiv pentru care principala dificultate o reprezintă trecerea de la 4G la 5G, practic instalarea tehnologiei 5G la nivelul întregii Uniuni Europene. Riscul de apariție a unui decalaj digital există întotdeauna, dar se preconizează ca acest risc să fie abordat ca o prioritate de politică în cadrul programului de politică „Calea către deceniul digital", în raport cu traiectoriile către atingerea, până în 2030, a țintei de acoperire 5G în proporție de 100 % a tuturor zonelor populate , sprijinind astfel statele membre să ia măsuri în acest domeniu, în special în ceea ce privește accesul la aceste rețele în zonele rurale.

32. Observatorul pentru 5G a reprezentat o sursă fiabilă de monitorizare a implementării rețelelor 5G în Uniunea Europeană și în afara acesteia, deși au apărut unele deficiențe. Serviciile Comisiei se așteaptă să dispună de mai multe informații actualizate din partea noului contractant.

Răspunsul comun al Comisiei la punctele 48 și 49:

Comisia consideră că alegerea instrumentului (recomandarea) și abordarea bazată pe colaborarea cu statele membre în vederea identificării riscurilor și a măsurilor de atenuare reprezintă cea mai adecvată cale de acțiune pentru a aborda în mod rapid, eficace și concertat riscurile de securitate legate de rețelele 5G.

Comisia a optat pentru o recomandare și pentru colaborarea cu statele membre în vederea identificării riscurilor și a măsurilor de atenuare, având în vederea complexitatea și caracterul transversal al subiectului în cadrul competențelor naționale și ale UE, precum și dimensiunea importantă a securității naționale. În plus, Comisia a ținut seama și de faptul că statele membre au contexte naționale foarte diferite (structura pieței, capacitățile de securitate cibernetică, informațiile privind amenințările etc).

Setul de instrumente al UE reprezintă un instrument dinamic bazat pe riscuri care permite abordarea provocărilor în materie de securitate și gestionarea în timp util și în mod eficient a aspectelor legate de securitatea cibernetică a rețelelor 5G.

În comunicarea sa intitulată „Implementarea rețelelor 5G în condiții de siguranță în UE - Punerea în aplicare a setului de instrumente al UE" din ianuarie 2020, Comisia a anunțat că va oferi sprijin pentru punerea în aplicare a măsurilor din setul de instrumente referitoare la cerințele de securitate, în special în ceea ce privește actele de punere în aplicare în care se detaliază măsurile de securitate tehnice și organizatorice necesare pentru completarea normelor naționale și sporirea eficacității și a coerenței măsurilor de securitate impuse operatorilor.

Răspunsul comun al Comisiei la punctele 51 și 52:

În contextul revizuirii recomandării Comisiei, care a avut loc în decembrie 2020, Comisia a purtat discuții cu autoritățile competente din toate statele membre. Acestea au considerat acțiunea coordonată a Europei cu privire la tehnologia 5G ca fiind una oportună, eficace și proporțională. Abordarea pe bază de colaborare între autoritățile naționale, Comisie, ENISA și alte părți interesate relevante a fost considerată adecvată pentru a aborda această problemă complexă. Acest lucru a favorizat definirea în timp util a unor obiective și metodologii comune, permițând, concomitent, statelor membre să își adapteze măsurile la circumstanțele lor naționale.

Setul de instrumente al UE și raportul intermediar publicat de Grupul de cooperare NIS în iulie 2020 recomandă definirea unor planuri de punere în aplicare și/sau a unor perioade de tranziție pentru acei

operatori care în prezent folosesc echipamente de la furnizori care prezintă un grad ridicat de risc sau pentru operatorii care au încheiat deja contracte cu astfel de furnizori înainte de adoptarea setului de instrumente al UE (de exemplu, ținând cont de ciclurile de modernizare a echipamentelor, în special de trecerea de la rețelele 5G care nu sunt de sine stătătoare la rețele de sine stătătoare).

55. Comisia ia notă de observațiile prezentate de Curtea de Conturi Europeană.

Pentru a sprijini în continuare punerea în aplicare a acestora, criteriile setului de instrumente pentru evaluarea furnizorilor cu grad ridicat de risc a făcut obiectul a numeroase schimburi între autoritățile naționale competente din cadrul Grupului de cooperare NIS, din momentul în care s-a ajuns la un acord cu privire la setul de instrumente al UE.

56. Setul de instrumente al UE recomandă ca, pentru evaluarea profilului de risc al furnizorilor, să se țină seama de factorii de risc prezentați în evaluarea coordonată a riscurilor la nivelul UE, precum și de informațiile specifice fiecărei țări (de exemplu, evaluarea amenințărilor din partea serviciilor naționale de securitate etc.).

61. Capacitatea furnizorului de a asigura aprovizionarea reprezintă unul dintre criteriile recomandate de setul de instrumente al UE pentru evaluarea profilului de risc al furnizorilor. Capacitatea de asigurare a aprovizionării ar putea fi afectată și de eventualele sancțiuni comerciale cu care s-ar putea confrunta un anumit furnizor, astfel cum se menționează în scenariul de risc privind „dependența” din evaluarea coordonată a riscurilor la nivelul UE.

Răspunsul comun al Comisiei la punctele 70 și 73:

În cadrul Grupului de cooperare NIS, Comisia și statele membre fac schimb de informații detaliate cu privire la punerea în aplicare a setului de instrumente la nivel național. Statelor membre le revine răspunderea de a face publice informații care nu au caracter public.

Răspunsul comun al Comisiei la punctele 74 până la 76 și la caseta 5:

Setul de instrumente al UE oferă un cadru pentru promovarea coerenței pe piața internă, cu respectarea concomitentă a competențelor naționale în materie de securitate în acest domeniu.

În ceea ce privește abordarea statelor membre față de furnizorii cu grad ridicat de risc, Comisia consideră că va fi posibil să se efectueze o evaluare concludentă numai atunci când vor fi disponibile mai multe informații.

Pe durata procesului de punere în aplicare, Comisia colaborează cu statele membre în cadrul Grupului de cooperare NIS, cu scopul de a promova alinierea și convergența abordărilor naționale.

CONCLUZII ȘI RECOMANDĂRI

81. Instalarea rapidă și sigură a rețelelor 5G reprezintă o prioritate majoră pentru Comisie. Protejarea rețelelor 5G împotriva amenințărilor cibernetice presupune evaluarea și atenuarea amenințărilor și riscurilor. Aceste amenințări și riscuri au fost identificate și evaluate în comun de statele membre, cu sprijinul Comisiei și al ENISA și, pornind de la această evaluare, au fost identificate o serie de măsuri cuprinzătoare pentru atenuarea riscurilor identificate. Deși în unele state membre lucrările sunt în curs, o mare parte a acestora au consolidat deja, pe baza setului de instrumente al UE, cerințele de securitate pentru rețelele 5G sau sunt în curs de consolidare a acestora:

Setul de instrumente al UE oferă un cadru cuprinzător pentru abordarea riscurilor legate de securitatea rețelelor 5G.

83. Tehnologia 5G reprezintă un „salt”, o schimbare majoră în comparație cu tehnologia 4G, astfel încât principala provocare pentru evitarea decalajului digital este tranziția de la 4G la 5G în întreaga UE.

Specificațiile privind rețelele 5G acoperă o gamă întreagă de indicatori de performanță, în special în ceea ce privește cazurile de utilizare verticală. Printre altele, acest lucru ar presupune cerințe de

fiabilitate, rapiditatea concretizării serviciului, flexibilitatea punerii în aplicare și niveluri de securitate.

Recomandarea 1 – Promovarea unei implementări uniforme și în timp util a rețelelor 5G în UE

a) Comisia acceptă recomandarea.

Comisia va colabora cu statele membre în vederea elaborării unei definiții comune a calității preconizate a serviciului furnizat de rețelele 5G. În contextul Deceniului digital și al propunerii de decizie privind programul de politică digitală pentru 2030, Comisia intenționează să colaboreze cu statele membre cu privire la o abordare comună a calității serviciului furnizat de rețelele 5G în UE, inclusiv pentru comparabilitatea măsurătorilor și a datelor de monitorizare.

Calitatea serviciului nu implică doar viteza și latența, ci acoperă și o gamă largă de indicatori de performanță, în special cei legați de cazurile de utilizare verticală.

Comisia își propune să colaboreze cu statele membre în scopul definirii unor astfel de măsurători, precum și în scopul efectuării unor verificări anuale și al recomandării de politici, măsuri și acțiuni în vederea asigurării unei acoperiri 5G complete până în 2030.

Programul de politică digitală va institui o guvernanță solidă prin intermediul unui mecanism de monitorizare și cooperare, în vederea asigurării progresului necesar pentru a îndeplini obiectivele programului de politică, inclusiv implementarea tehnologiei 5G, și va recomanda statelor membre să ia măsuri de remediere în acest sens.

b) Comisia acceptă recomandarea.

c) Comisia acceptă recomandarea.

Recomandarea 2 – Promovarea unei abordări concertate între statele membre în ceea ce privește securitatea rețelelor 5G

a) Comisia acceptă recomandarea.

Împreună cu statele membre, Comisia va efectua o evaluare a necesității unor acțiuni sau a unor măsuri de sprijin suplimentare, de pildă sub forma unor îndrumări cu privire la anumite aspecte ale setului de instrumente al UE.

b) Comisia acceptă recomandarea.

Exercițiul de monitorizare și raportare va fi realizat de Comisie, în deplină colaborare cu statele membre și cu ENISA.

c) Comisia acceptă recomandarea.

Recomandarea 3 – Examinarea impactului pe care abordările divergente ale statelor membre în materie de securitate a rețelelor 5G îl au asupra eficacității funcționării pieței unice

a) Comisia acceptă recomandarea.

b) Comisia acceptă recomandarea.

Comisia va efectua evaluarea ținând seama de competențele naționale.

În cadrul setului de instrumente al UE, este de competența statelor membre să decidă cu privire la domeniul de aplicare exact al restricțiilor adecvate și/sau cu privire la excluderile necesare pentru activele-cheie definite ca fiind critice și sensibile în evaluarea coordonată a riscurilor la nivelul UE (de exemplu funcțiile de rețea magistrală, cele de administrare și orchestrare a rețelei și funcțiile de acces la rețea), pentru a atenua în mod eficace riscurile, ținând cont și de evaluările amenințărilor puse la dispoziție de către serviciile naționale de informații. Statele membre au dreptul de a lua măsuri

legate de securitatea națională, inclusiv eventuale restricții sau excluderi ale vânzătorilor cu grad ridicat de risc.