RECOMANDĂRI

RECOMANDAREA (UE) 2019/534 A COMISIEI

din 26 martie 2019

Securitatea cibernetică a rețelelor 5G

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 292,

întrucât:

(1) Comisia a recunoscut că implementarea tehnologiilor de rețea de generația a 5-a (5G) este atât un factor major care facilitează serviciile digitale viitoare, cât și o prioritate pentru Strategia privind piața unică digitală. Pentru a se asigura că Uniunea dispune de infrastructura de conectivitate necesară transformării sale digitale începând cu 2020, Comisia a adoptat Planul de acțiune privind 5G ([1]).

(2) Rețelele 5G se vor dezvolta pornind de la tehnologiile de rețea actuale de generația a 4-a (4G), prin furnizarea de noi capacități de prestare de servicii, devenind astfel infrastructura centrală și catalizatorul principal pentru o mare parte a economiei Uniunii. După ce vor fi implementate, rețelele 5G vor sta la baza unei game variate de servicii esențiale pentru funcționarea pieței interne și pentru întreținerea și operarea unor funcții vitale ale societății și economiei – de exemplu, sistemele energetice, de transport, bancare și medicale, precum și sistemele de control industrial. Organizarea proceselor democratice, cum ar fi alegerile, se vor baza tot mai mult pe infrastructura digitală și pe rețelele 5G.

(3) Întrucât multe servicii fundamentale ar fi dependente de rețelele 5G, în cazul unor perturbări sistemice la scară largă, consecințele ar fi deosebit de grave. Prin urmare, asigurarea securității cibernetice a rețelelor 5G este o chestiune de o importanță strategică pentru Uniune, în momentul în care atacurile cibernetice sunt în creștere și mai sofisticate ca niciodată.

(4) Datorită interconectării și caracterului transnațional al infrastructurilor aflate la baza ecosistemului digital, precum și naturii transfrontaliere a amenințărilor implicate, orice vulnerabilitate și/sau incident de securitate cibernetică de amploare care vizează rețelele 5G și care se produce într-un stat membru ar afecta Uniunea în ansamblul său. Acesta este motivul pentru care ar trebui prevăzute măsuri care să stea la baza unui nivel comun ridicat de securitate cibernetică a rețelelor 5G.

(5) Statele membre au confirmat necesitatea unei acțiuni la nivelul Uniunii. Potrivit concluziilor sale din 21 martie 2019, Consiliul European așteaptă cu interes o recomandare a Comisiei privind o abordare concertată a securității rețelelor 5G ([2]).

(6) Asigurarea suveranității europene ar trebui să fie un obiectiv major, cu respectarea deplină a valorilor de deschidere și toleranță ale Europei ([3]). Investițiile străine în sectoarele strategice, achiziționarea de active, tehnologii și infrastructuri critice în Uniune și furnizarea de echipamente esențiale pot, de asemenea, reprezenta riscuri la adresa securității Uniunii.

(7) Securitatea cibernetică a rețelelor 5G este esențială pentru asigurarea autonomiei strategice a Uniunii, astfel cum se recunoaște în Comunicarea comună „UE-China – o perspectivă strategică” ([4]).

(8) Totodată, prin Rezoluția Parlamentului European referitoare la amenințările la adresa securității în legătură cu prezența tehnologică în creștere a Chinei în UE, Comisia și statele membre sunt invitate să ia măsuri la nivelul Uniunii ([5]).

(9) Prezenta recomandare abordează riscurile la adresa securității cibernetice a rețelelor 5G, prin formularea unor orientări privind analiza de risc și măsurile de gestionare adecvate la nivel național, prin pregătirea unei evaluări coordonate a riscurilor la nivel european și prin stabilirea unui proces de elaborare a unui set comun de instrumente care să cuprindă cele mai bune măsuri de gestionare a riscurilor.

(10) Uniunea dispune de un cadru legislativ solid care asigură protecția rețelelor de comunicații electronice.

([1]) COM(2016) 588 final.
([2]) Concluziile Consiliului European din 21 și 22 martie 2019.
([3]) Starea Uniunii 2018 – Ora suveranității europene, 12 septembrie 2018.
([4]) JOIN(2019) 5 final.
([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//RO.

(11) Cadrul Uniunii în domeniul comunicațiilor electronice ([6]) promovează concurența, piața internă și interesele utilizatorilor finali și, împreună cu Codul european al comunicațiilor electronice ([7]), urmărește un obiectiv suplimentar în materie de conectivitate, definit din perspectiva rezultatelor, și anume: implementarea pe scară largă a unei conectivități fixe și mobile de foarte mare capacitate și accesul tuturor cetățenilor și al întreprinderilor din Uniune la aceasta, în paralel cu protecția intereselor cetățenilor. Directiva 2002/21/CE impune statelor membre să asigure menținerea integrității și securității rețelelor de comunicații publice, întreprinderile care furnizează rețele de comunicații publice sau servicii de comunicații electronice accesibile publicului având obligația de a lua măsuri tehnice și organizatorice pentru a gestiona în mod corespunzător riscurile la adresa securității rețelelor și serviciilor. Directiva respectivă prevede, de asemenea, că autoritățile naționale de reglementare în domeniu au competențe, inclusiv competența de a emite instrucțiuni obligatorii, pentru a asigura respectarea acestor obligații.

(12) În plus, Directiva 2002/20/CE a Parlamentului European și a Consiliului ([8]) permite statelor membre să stabilească condiții privind siguranța rețelelor publice care să împiedice accesul neautorizat la autorizația generală, în scopul protejării confidențialității comunicațiilor în conformitate cu Directiva 2002/58/CE a Parlamentului European și a Consiliului ([9]).

(13) Pentru a sprijini punerea în aplicare a acestor obligații, Uniunea a instituit o serie de organisme de cooperare. Agenția pentru Securitatea Rețelelor și a Informațiilor (ENISA), Comisia, statele membre și autoritățile naționale de reglementare au elaborat pentru acestea din urmă orientări tehnice cu privire la raportarea incidentelor, măsurile de securitate, amenințări și active ([10]). Grupul de cooperare instituit prin Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului ([11]) („grupul de cooperare") reunește autorități competente cu scopul de a sprijini și a facilita cooperarea, în special prin furnizarea de orientări strategice pentru activitățile rețelei formate din echipe de intervenție în caz de incidente de securitate informatică, care, la nivel tehnic, susține cooperarea operațională.

(14) Viitorul cadru european de certificare de securitate cibernetică ([12]) ar trebui să asigure un instrument de sprijin esențial pentru promovarea unor niveluri consecvente de securitate. Cadrul respectiv ar trebui să permită dezvoltarea unor sisteme de certificare de securitate cibernetică care să răspundă nevoilor utilizatorilor de echipamente și software 5G. Dată fiind importanța crucială a acestor infrastructuri, o prioritate imediată ar trebui să fie dezvoltarea unor sisteme europene relevante de certificare de securitate cibernetică pentru produsele, serviciile sau procesele din domeniul tehnologiilor informației și comunicațiilor utilizate pentru rețelele 5G. Statele membre și actorii de pe piață ar trebui să se implice în mod activ în dezvoltarea unor astfel de sisteme de certificare, inclusiv sprijinind definirea unor profiluri specifice de protecție pentru rețelele 5G.

(15) În absența unei legislații armonizate a Uniunii, statele membre pot prevedea, prin intermediul unor reglementări tehnice naționale, adoptate în conformitate cu dreptul Uniunii, faptul că un sistem european de certificare de securitate cibernetică ar trebui să fie obligatoriu. Statele membre recurg, de asemenea, la sistemele europene de certificare de securitate cibernetică în contextul achizițiilor publice și al Directivei 2014/24/UE a Parlamentului European și a Consiliului ([13]) și ar putea susține dezvoltarea unor mecanisme de asistență – cum ar fi un centru de asistență – astfel încât achizitorii publici să cumpere soluții de securitate cibernetică.

(16) Un nivel ridicat de protecție a datelor și a vieții private este un element important în asigurarea securității rețelelor 5G. De asemenea, la nivelul Uniunii au fost definite norme care asigură securitatea prelucrării datelor cu caracter personal, inclusiv în comunicațiile electronice. Regulamentul general privind protecția datelor ([14]) stabilește obligația de a prelucra datele cu caracter personal într-un mod care să le asigure securitatea, inclusiv pentru prevenirea accesului neautorizat la datele cu caracter personal și la echipamentul utilizat pentru prelucrare ori a utilizării neautorizate a datelor sau a echipamentului respectiv. Directiva asupra confidențialității și

([6]) Directiva 2002/21/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice (Directivă-cadru) (JO L 108, 24.4.2002, p. 33) și directivele specifice.

([7]) Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice (JO L 321, 17.12.2018, p. 36).

([8]) Directiva 2002/20/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind autorizarea rețelelor și serviciilor de comunicații electronice (Directiva privind autorizarea) (JO L 108, 24.4.2002, p. 21).

([9]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

([10]) https://resilience.enisa.europa.eu/article-13.

([11]) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194, 19.7.2016, p. 1).

([12]) Propunere de regulament al Parlamentului European și al Consiliului privind ENISA, „Agenția UE pentru securitate cibernetică", de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Legea privind securitatea cibernetică"), [COM(2017) 477 final – 2017/0225 (COD)].

([13]) Directiva 2014/24/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile publice și de abrogare a Directivei 2004/18/CE (JO L 94, 28.3.2014, p. 65).

([14]) 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) (JO L 119, 4.5.2016, p. 1).

comunicațiilor electronice stabilește norme specifice privind protecția confidențialității comunicațiilor și a echipamentelor terminale ale utilizatorilor finali. De asemenea, directiva respectivă impune prestatorilor de servicii obligația de a lua măsurile tehnice și organizatorice adecvate pentru a garanta securitatea serviciilor lor.

(17) Uniunea a adoptat, de asemenea, un instrument care va proteja infrastructura și tehnologiile critice, cum ar fi cele utilizate în domeniul comunicațiilor, întrucât va permite statelor membre să examineze investițiile străine directe din perspectiva securității sau a ordinii publice și va crea un mecanism de cooperare în cadrul căruia statele membre și Comisia vor putea să facă schimb de informații și să își exprime preocupările legate de anumite investiții ([15]).

(18) Statele membre și operatorii adoptă în prezent măsuri pregătitoare importante în vederea introducerii pe scară largă a rețelelor 5G. Mai multe state membre și-au exprimat îngrijorarea cu privire la potențialele riscuri la adresa securității rețelelor 5G în contextul derulării procedurilor de acordare a drepturilor de utilizare în benzile de frecvențe radio desemnate pentru rețelele 5G ([16]) și au analizat măsuri de contracarare a acestor riscuri.

(19) Pentru a răspunde riscurilor la adresa securității cibernetice cu care se confruntă rețelele 5G ar trebui să se țină seama atât de factori tehnici, cât și de factori de altă natură. Printre factorii tehnici se pot număra vulnerabilitățile în materie de securitate cibernetică ce ar putea fi exploatate pentru a obține acces neautorizat la informații (spionaj cibernetic, din motive economice sau politice) sau în alte scopuri rău intenționate (atacuri cibernetice menite să perturbe sau să distrugă sisteme și date). Ar trebui să se ia în considerare aspecte importante, cum ar fi necesitatea de a proteja rețelele de-a lungul întregului lor ciclu de viață, precum și necesitatea de a cuprinde toate echipamentele relevante, inclusiv în fazele de proiectare, dezvoltare, achiziții, implementare, operare și întreținere ale rețelelor 5G.

(20) Printre factorii de altă natură se pot număra cerințele de reglementare sau alte cerințe impuse furnizorilor de echipamente de tehnologie a informației și comunicațiilor. La evaluarea importanței acestor factori ar trebui să se țină seama, printre altele, de riscul general pe care îl are influența din partea unei țări terțe, în special în ceea ce privește modelul său de guvernanță, de lipsa unor acorduri de cooperare în materie de securitate ori a unor acorduri similare – de exemplu decizii privind caracterul adecvat al nivelului de protecție – referitoare la protecția datelor încheiate între Uniune și țara terță în cauză sau de faptul că țara respectivă este ori nu parte la acorduri multilaterale, internaționale sau bilaterale privind securitatea cibernetică, combaterea criminalității informatice ori protecția datelor.

(21) Un pas important în dezvoltarea unei abordări la nivelul Uniunii cu privire la securitatea cibernetică a rețelelor 5G ar trebui să fie realizarea și finalizarea la nivel național a unei evaluări a riscurilor. Astfel, în urma acestei evaluări, statele membre și-ar putea adapta măsurile naționale privind cerințele de securitate și gestionarea riscurilor.

(22) Ar trebui consolidată coordonarea pentru a se asigura eficacitatea măsurilor care vizează combaterea acestor amenințări la adresa securității cibernetice; măsurile respective sunt esențiale pentru buna funcționare a pieței interne și pentru protecția datelor cu caracter personal și a vieții private.

(23) Evaluările naționale ale riscurilor ar trebui să stea la baza unei evaluări coordonate a riscurilor la nivelul Uniunii, alcătuite dintr-o cartografiere a amenințărilor și o revizuire comună care urmează să fie efectuată de statele membre, cu sprijin din partea Comisiei și împreună cu Agenția Europeană pentru Securitate Cibernetică (ENISA).

(24) Ținând seama de evaluările riscurilor la nivel național și la nivelul Uniunii, grupul de cooperare ar trebui să elaboreze un set de instrumente de identificare a tipurilor de riscuri în materie de securitate cibernetică și a eventualelor măsuri de atenuare a riscurilor în domenii precum certificarea, testarea și controalele accesului. De asemenea, acest grup ar trebui să identifice posibile măsuri specifice adecvate pentru a răspunde riscurilor identificate de unul sau mai multe state membre. Grupul de cooperare ar trebui să se bazeze pe sprijinul oferit de Agenția Europeană pentru Securitate Cibernetică (ENISA), de Europol, de Organismul Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice (OAREC) și de Centrul de situații și de analiză a informațiilor al UE. Acest set de instrumente ar trebui să ofere consiliere Comisiei cu privire la elaborarea unor cerințe comune minime pentru a asigura în continuare un nivel ridicat de securitate cibernetică a rețelelor 5G în întreaga Uniune.

(25) Atunci când se iau măsuri care să răspundă riscurilor de securitate cibernetică, ar trebui să se acorde atenție promovării securității cibernetice prin utilizarea unei game largi de furnizori la construcția oricărei rețele unice.

([15]) Regulamentul (UE) 2019/452 al Parlamentului European și al Consiliului din 19 martie 2019 de stabilire a unui cadru pentru examinarea investițiilor străine directe în Uniune (JO L 79 I, 21.3.2019, p. 1).

([16]) Procedura de licitație pentru cel puțin o bandă de frecvențe este programată a avea loc în 2019 în următoarele 11 state membre: Austria, Belgia, Cehia, Franța, Germania, Grecia, Ungaria, Irlanda, Țările de Jos, Lituania, Portugalia. Pentru 2020 sunt programate alte șase licitații în: Spania, Malta, Lituania (frecvențe diferite), Slovacia, Polonia, Regatul Unit. Sursă: http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) Prezenta recomandare nu ar trebui să aducă atingere competențelor statelor membre în ceea ce privește activitățile de siguranță publică, apărare, securitate națională și activitățile statului în domeniul dreptului penal, nici dreptului statelor membre de a exclude prestatorii sau furnizorii de pe piețele lor din motive de securitate națională,

ADOPTĂ PREZENTA RECOMANDARE:

I. **OBIECTIVE**

1. Pentru a sprijini elaborarea la nivelul Uniunii a unei abordări cu privire la asigurarea securității cibernetice a rețelelor 5G, prezenta recomandare identifică acțiunile care ar trebui întreprinse pentru a permite:

   (a) statelor membre să evalueze riscurile de securitate cibernetică ce afectează rețelele 5G la nivel național și să ia măsurile de securitate necesare;

   (b) statelor membre și instituțiilor, agențiilor și altor organisme relevante ale Uniunii să efectueze în comun o evaluare coordonată a riscurilor la nivelul Uniunii, care să se bazeze pe evaluarea riscurilor la nivel național;

   (c) grupului de cooperare instituit în temeiul Directivei (UE) 2016/1148 (grupul de cooperare) să identifice un posibil set comun de măsuri care să fie luate pentru a atenua riscurile de securitate cibernetică legate de infrastructurile aflate la baza ecosistemului digital, în special rețelele 5G.

II. **DEFINIȚII**

2. În sensul prezentei recomandări:

   (a) „rețele 5G” înseamnă un set format din toate elementele relevante ale infrastructurilor de rețea pentru tehnologia de comunicații mobile și fără fir utilizată pentru conectivitate și servicii cu valoare adăugată cu caracteristici de performanță avansată, cum ar fi rate și capacitate de date foarte mari, comunicații cu latență mică, fiabilitate extrem de ridicată sau acceptarea unui număr mare de dispozitive conectate. Printre acestea se pot număra elemente ale rețelei tradiționale, bazate pe tehnologii de comunicații mobile și fără fir din generații anterioare, precum 4G sau 3G. Rețelele 5G ar trebui înțelese ca incluzând toate părțile relevante ale rețelei;

   (b) „infrastructuri aflate la baza ecosistemului digital” înseamnă infrastructuri utilizate pentru a permite digitalizarea într-o gamă largă de aplicații esențiale în economie și societate.

III. **ACȚIUNEA LA NIVELUL UE**

3. Până la 30 iunie 2019, statele membre ar trebui să efectueze o evaluare a riscurilor legate de infrastructura rețelelor 5G, care să cuprindă și identificarea celor mai sensibile elemente în cazul cărora încălcările normelor de securitate ar avea un impact negativ semnificativ. Până la aceeași dată, statele membre ar trebui să revizuiască, de asemenea, cerințele de securitate și metodele de gestionare a riscurilor aplicabile la nivel național, pentru a lua în considerare amenințările la adresa securității cibernetice care ar putea rezulta din (i) factorii tehnici, cum ar fi caracteristicile tehnice specifice ale rețelelor 5G, și din (ii) factori de altă natură, precum cadrul juridic și de politică sub incidența căruia pot intra furnizorii de echipamente de tehnologia informației și comunicațiilor din țări terțe.

4. Pe baza acestei evaluări naționale a riscurilor și a revizuirii menționate și luând în considerare acțiunea coordonată aflată în derulare la nivelul Uniunii, statele membre ar trebui:

   (a) să actualizeze cerințele de securitate și metodele de gestionare a riscurilor aplicate în ceea ce privește rețelele 5G;

   (b) să actualizeze obligațiile relevante impuse întreprinderilor care furnizează rețele de comunicații publice sau servicii de comunicații electronice accesibile publicului în conformitate cu articolele 13a și 13b din Directiva 2002/21/CE;

   (c) să stabilească condiții pentru autorizația generală privind siguranța rețelelor publice care să împiedice accesul neautorizat și să solicite angajamente din partea întreprinderilor care participă la eventuale proceduri viitoare de acordare a drepturilor de utilizare a frecvențelor radio în benzile 5G în ceea ce privește respectarea cerințelor de securitate pentru rețele, în temeiul Directivei 2002/20/CE;

   (d) să aplice alte măsuri preventive menite să atenueze riscurile potențiale în materie de securitate cibernetică.

5. Printre măsurile menționate la punctul 4 ar trebui să se numere mai multe obligații pentru furnizori și operatori de a asigura securitatea elementelor sensibile ale rețelelor, precum și alte obligații, după caz, de exemplu de a pune la dispoziția autorităților naționale competente informații relevante cu privire la modificările planificate ale rețelelor de comunicații electronice, precum și cerințe pentru ca laboratoarele naționale de audit/certificare să testeze, în prealabil, din motive de securitate și integritate, anumite componente și sisteme de tehnologie a informației.

6. Revizuirile comune de securitate ar trebui efectuate de două sau mai multe state membre, utilizând și împărtășind expertiza tehnică adecvată și facilitățile legate de infrastructurile aflate la baza ecosistemului digital și a rețelelor 5G, de exemplu în cazul în care aceeași întreprindere operează sau dezvoltă infrastructura de rețea în mai multe state membre sau în cazul în care există similitudini importante între configurațiile rețelelor. Agenția Europeană pentru Securitate Cibernetică (ENISA), Europol și Organismul Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice (OAREC) ar trebui să acorde prioritate cererilor de sprijin adresate de statele membre în acest domeniu. Rezultatele acestor revizuiri ar trebui transmise grupului de cooperare și rețelei echipelor de intervenție în caz de incidente de securitate informatică.

IV. **ACȚIUNEA COORDONATĂ LA NIVELUL UNIUNII**

7. Pentru a avea o abordare comună care să răspundă riscurilor la adresa securității cibernetice a rețelelor 5G, statele membre ar trebui să înceapă să acționeze, până la 30 aprilie 2019, în cadrul unui flux de lucru specific al grupului de cooperare. Statele membre ar trebui să invite autoritățile relevante să participe, dacă este cazul, la lucrările grupului de cooperare.

O evaluare coordonată a riscurilor la nivel european

8. Statele membre ar trebui să facă schimb de informații între ele și cu organismele competente ale Uniunii pentru a dezvolta un bagaj comun de cunoștințe privind riscurile de securitate cibernetică existente și potențiale asociate rețelelor 5G.

9. Până la 15 iulie 2019, statele membre ar trebui să transmită Comisiei și Agenției Europene pentru Securitatea Cibernetică (ENISA) evaluările lor naționale ale riscurilor.

10. Agenția Europeană pentru Securitate Cibernetică (ENISA) ar trebui să finalizeze cartografierea specifică a amenințărilor la adresa rețelelor 5G. Grupul de cooperare și rețeaua echipelor de intervenție în caz de incidente de securitate informatică, înființate în temeiul Directivei (UE) 2016/1148, ar trebui să sprijine acest proces.

11. Ținând seama de toate aceste elemente, până la 1 octombrie 2019, statele membre, cu sprijinul Comisiei și împreună cu Agenția Europeană pentru Securitate Cibernetică (ENISA), ar trebui să finalizeze o revizuire comună a expunerii la nivelul Uniunii la riscurile legate de infrastructurile aflate la baza ecosistemului digital, în special rețelele 5G.

12. Această revizuire comună ar trebui să acorde prioritate unei analize a riscurilor aplicabile elementelor deosebit de sensibile sau vulnerabile incluse în elementele principale ale rețelelor 5G, centrului de operare și de întreținere, precum și elementelor de rețea privind accesul la tehnologia 5G utilizate pentru aplicații industriale.

13. Într-o a doua etapă, această revizuire comună ar trebui extinsă la alte elemente strategice ale lanțului valoric digital.

Un set de instrumente comune la nivelul Uniunii pentru contracararea riscurilor

14. Activitatea grupului de cooperare ar trebui să identifice măsurile privind cele mai bune practici aplicate la nivel național, de tipul celor prevăzute la punctul 4. Pe baza acestor bune practici naționale, până la 31 decembrie 2019 ar trebui să se convină asupra unui set de instrumente care să vizeze măsuri adecvate, eficace și proporționale de gestionare a riscurilor posibile pentru a reduce riscurile în materie de securitate cibernetică identificate la nivel național și la nivelul Uniunii; scopul este acela de a oferi consultanță Comisiei cu privire la elaborarea unor cerințe comune minime, menite să asigure în continuare un nivel ridicat de securitate cibernetică a rețelelor 5G în întreaga Uniune.

15. Acest set de instrumente ar trebui să cuprindă:

(a) un inventar al tipurilor de riscuri de securitate care pot afecta securitatea cibernetică a rețelelor 5G (de exemplu, riscul aferent lanțului de aprovizionare, riscul de vulnerabilitate pentru software, riscul de control al accesului, riscurile care decurg din cadrul juridic și de politică sub incidența căruia pot intra furnizorii de echipamente de tehnologia informației și comunicațiilor în țări terțe), precum și

(b) o serie de măsuri posibile de atenuare (de exemplu, certificarea de către terți pentru hardware, software sau servicii, teste oficiale sau verificări ale conformității pentru hardware și software, proceduri prin care să se asigure existența și aplicarea unor controale ale accesului, identificarea produselor, serviciilor sau furnizorilor care sunt considerați potențial nesiguri etc.). Aceste măsuri ar trebui să abordeze fiecare tip de risc de securitate identificat în unul sau mai multe state membre în urma evaluării riscurilor.

16. După instituirea sistemelor europene de certificare de securitate cibernetică relevante pentru rețelele 5G, statele membre ar trebui să adopte, în conformitate cu dreptul Uniunii, reglementări tehnice naționale care să prevadă certificarea obligatorie a produselor, serviciilor sau sistemelor de tehnologie a informației și comunicațiilor care sunt acoperite de aceste sisteme de certificare.

17. Statele membre, împreună cu Comisia, ar trebui să identifice condițiile legate de siguranța rețelelor publice menite să împiedice accesul neautorizat care ar trebui să fie respectate pentru obținerea autorizației generale și cerințele de securitate pentru rețele, scopul fiind acela de a solicita angajamente din partea întreprinderilor care participă la procedurile de acordare a drepturilor de utilizare a spectrului în benzile 5G, în temeiul Directivei 2002/20/CE. Aceste cerințe ar trebui să se reflecte, dacă este posibil, în măsurile luate la punctul 4 litera (c).

18. Statele membre ar trebui să coopereze cu Comisia pentru a elabora cerințe de securitate specifice care ar putea fi aplicate în contextul achizițiilor publice legate de rețelele 5G. Printre aceste cerințe ar trebui să se numere cerințe obligatorii de introducere a sistemelor de certificare de securitate cibernetică în domeniul achizițiilor publice, în măsura în care aceste sisteme nu sunt încă obligatorii pentru toți furnizorii și operatorii.

V. **REVIZUIREA**

19. Statele membre ar trebui să coopereze cu Comisia pentru a evalua efectele prezentei recomandări până la 1 octombrie 2020, cu scopul de a stabili căile adecvate de urmat. Această analiză ar trebui să țină seama de rezultatul evaluării coordonate a riscurilor la nivelul Uniunii și de setul de instrumente al Uniunii.

Adoptată la Strasbourg, 26 martie 2019.

Pentru Comisie
Julian KING
Membru al Comisiei