ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații

Str. Delea Nouă nr.2, Sector 3, 030925 București, România
Telefon: 0372 845 400 / 0372 845 454. Fax: 0372 845 402
E-mail: ancom@ancom.ro. Website: www.ancom.ro

SINTEZA OBSERVAȚIILOR
la
Proiectul de decizie a Autorității Naționale pentru Administrare și Reglementare în Comunicații privind securitatea rețelelor publice de comunicații electronice și a serviciilor de comunicații electronice destinate publicului

Perioada de consultare pentru Proiectul de decizie a Autorității Naționale pentru Administrare și Reglementare în Comunicații privind securitatea rețelelor publice de comunicații electronice și a serviciilor de comunicații electronice destinate publicului (*Proiectul*), publicat pe pagina de internet a Autorității Naționale pentru Administrare și Reglementare în Comunicații (denumită în continuare *ANCOM* sau *Autoritatea*) în data de 01 august 2023, s-a încheiat în data de 08 septembrie 2023.

Proiectul de act normativ care a fost supus consultării publice urmărește stabilirea măsurilor tehnice și organizatorice care trebuie luate de furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului pentru a gestiona în mod corespunzător riscurile la adresa securității rețelelor și serviciilor de comunicații electronice, precum și a circumstanțelor, formatului și procedurilor aplicabile notificării ANCOM a unui incident de securitate care are un impact semnificativ asupra rețelelor sau serviciilor de comunicații electronice. În cadrul acestui demers, Autoritatea a pornit de la cadrul normativ actual, reprezentat de Decizia președintelui ANCOM nr. 512/2013[1]. Acest cadru a fost revizuit atât prin prisma evoluției tehnologiilor de comunicații electronice, cât și a experienţei dobândite în aplicarea acestuia de la intrarea în vigoare în anul 2013. În același timp, au fost avute în vedere dispozițiile actelor normative cu caracter primar și, nu în ultimul rând, evoluția vulnerabilităților și a amenințărilor la adresa securității rețelelor și serviciilor de comunicații electronice.

Astfel, prezentul demers al Autorității a avut în vedere implementarea unor elemente de noutate apărute în legislația primară – Ordonanţa de urgenţă a Guvernului nr. 111/2011[2] – cu ocazia transpunerii Directivei (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice, transpunere realizată prin intermediul Legii nr. 198/2022 pentru modificarea și completarea unor acte normative în domeniul comunicațiilor electronice și pentru stabilirea unor măsuri de facilitare a dezvoltării rețelelor de comunicații electronice.

Au fost supuse consultării publice următoarele documente:

a) expunerea de motive la proiectul Deciziei Autorității Naționale pentru Administrare și Reglementare în Comunicații privind securitatea rețelelor publice de comunicații electronice și a serviciilor de comunicații electronice destinate publicului;

b) proiectul Deciziei Autorității Naționale pentru Administrare și Reglementare în Comunicații privind securitatea rețelelor publice de comunicații electronice și a serviciilor de comunicații electronice destinate publicului.

[1] Decizia președintelui ANCOM nr. 512/2013 privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului şi raportarea incidentelor cu impact semnificativ asupra furnizării reţelelor şi serviciilor de comunicaţii electronice.
[2] Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicaţiile electronice, aprobată, cu modificări şi completări, prin Legea nr. 140/2012, cu modificările şi completările ulterioare.

În conformitate cu prevederile art. 135 alin. (4) din Ordonanţa de urgenţă a Guvernului nr. 111/2011, ANCOM are obligaţia de a publica, pe pagina sa de internet, un material de sinteză a observaţiilor primite cu privire la măsurile supuse consultării, cu respectarea principiului confidențialității, în care va preciza şi poziţia sa faţă de aceste observaţii.

În cursul procedurii de consultare ANCOM a primit observații de la un număr de șase respondenți, principalele observații referindu-se la următoarele aspecte:

I. Observații privind incidentele care au un impact semnificativ și procesul de raportare a acestora

1. Un respondent solicită **eliminarea art. 2 alin. (1) pct. 5, litera b), subpunctele (i), (ii) şi (iv) din Proiect, care prevăd trei tipuri de praguri calitative** pe baza cărora se stabilesc o parte dintre incidentele care au un impact semnificativ și care trebuie raportate Autorității.

Primul dintre acestea vizează incidentele ce afectează direct sau indirect, pe o perioadă de cel puțin 15 minute, rutarea comunicațiilor de urgență către Serviciul de urgență 112. Respondentul informează ANCOM despre faptul că, în cazul unor astfel de incidente, există deja instituit un protocol de comunicare directă între furnizorii de comunicații electronice și Serviciul de Telecomunicații Speciale (STS) prin SNUAU, prin care se oferă suport dedicat în cazul incidentelor de natură să afecteze comunicațiile de urgență, iar introducerea unor obligații de notificare către ANCOM nu aduce niciun beneficiu practic în vederea gestionării şi remedierii unor astfel de incidente, doar implicând alocarea unor resurse suplimentare din partea operatorilor.

Cel de-al doilea element solicitat a fi eliminat din Proiect presupune trimiterea de către furnizori a unei notificări în cazul incidentelor care afectează furnizarea serviciilor de comunicații critice, respondentul afirmând că doar STS, în calitate de furnizor al serviciilor de comunicații critice, deține informațiile relevante cu privire la modul și perioada desfășurării unui incident care afectează propriile servicii pe care le furnizează, iar furnizorii de comunicații electronice nu au niciun fel de relație contractuală sau de altă natură cu autoritățile către care STS furnizează serviciile critice.

Pentru cel de-al treilea element, respondentul a motivat solicitarea de eliminare a pragului care determină notificarea de către furnizori a incidentelor ce afectează operatorii de servicii esențiale prin faptul că aceștia nu dețin informații cu privire la lista acestor operatori, neavând acces la Registrul Operatorilor de Servicii Esențiale (ROSE) şi nu pot raporta astfel de incidente.

Răspunsul ANCOM:

În urma analizei solicitării referitoare la eliminarea subpunctelor (i), (ii) și (iv) aferente literei b) de la pct. 5, alin. (1) al art. 2 din Proiect, care se referă la praguri calitative a căror îndeplinire implică transmiterea unei notificări către ANCOM, **cu privire la pragul ce vizează incidentele ce afectează direct sau indirect, pe o perioadă de cel puțin 15 minute, rutarea comunicațiilor de urgență către Serviciul de urgență 112**, ANCOM reiterează faptul că acesta a fost inclus pentru a asigura o monitorizare adecvată și o raportare transparentă a incidentelor care pot afecta rutarea comunicațiilor de urgență către Serviciul de urgență 112. Dată fiind importanța aparte a serviciului de urgență 112, acest prag calitativ a fost stabilit la un nivel adecvat acesteia. Poziția Autorității cu privire la acest prag calitativ pornește de la următoarele prevederi legale:

- conform art. 70 alin. (5) din Ordonanța de urgență a Guvernului nr. 111/2011: *„(5) Furnizorii de rețele publice de comunicații electronice au obligația de a asigura rutarea comunicațiilor de urgență către numărul european unic de urgență 112 ori către alte numere naționale de urgență, conform cadrului legislativ național privind organizarea și funcționarea Sistemului național unic pentru apeluri de urgență, indiferent dacă aceste comunicații de urgență sunt inițiate în rețeaua proprie sau în alte rețele publice de comunicații electronice, în măsura în care pentru alte comunicații de urgență decât apelurile, rutarea este tehnic fezabilă. Rutarea comunicațiilor de urgență către numărul european unic de urgență 112 ori către alte numere naționale de urgență va fi asigurată cu prioritate, conform prevederilor Ordonanței de urgență a Guvernului nr. 34/2008, aprobată cu modificări și completări prin Legea nr. 160/2008, cu modificările și completările ulterioare."*

- conform art. 14 lit. a) din Ordonanța de urgență a Guvernului nr. 34/2008[3]: *„Art. 14 – Furnizorii de servicii de comunicații interpersonale bazate pe numere, destinate publicului, care asigură prin*

[3] Ordonanța de urgență a Guvernului nr. 34/2008 privind organizarea și funcționarea Sistemului național unic pentru apeluri de urgență, aprobată cu modificări și completări prin Legea nr. 160/2008, cu modificările și completările ulterioare.

intermediul reţelelor publice fixe servicii de originare a apelurilor către un număr sau numere din Planul naţional de numerotaţie ori din planurile de numerotaţie internaţionale, au următoarele obligaţii: a) de a asigura, cu prioritate, primirea şi rutarea către cel mai adecvat PSAP a apelului de urgenţă de la orice post telefonic fix pe care îl operează până la deconectarea circuitului telefonic respectiv;.

Potrivit art. 15 lit. a) al aceluiași act normativ, *„Art. 15 - Furnizorii de servicii de comunicaţii interpersonale bazate pe numere, destinate publicului, care asigură prin intermediul reţelelor publice mobile servicii de originare a apelurilor către un număr sau numere din Planul naţional de numerotaţie ori din planurile de numerotaţie internaţionale, au următoarele obligaţii: a) de a asigura, cu prioritate, primirea și rutarea către cel mai adecvat PSAP a apelului de urgență, de la orice echipament terminal, indiferent de tipul de serviciu folosit de utilizatorul respectiv, inclusiv în cazurile în care utilizatorii finali se află în roaming pe teritoriul României;".*

- conform art. 21 alin. (1) din Decizia președintelui ANCOM nr. 1023/2008[4] : *„(1) Furnizorii de rețele publice de comunicații electronice au obligația de a lua toate măsurile necesare pentru a asigura în mod neîntrerupt transmiterea apelurilor către serviciul de urgență 112, prin utilizarea serviciilor de tranzit comutat furnizate de Operator, inclusiv în cazurile în care utilizatorii finali se află în roaming pe teritoriul României.*". Mai mult, conform alin. (2) din același articol, *„(2) Furnizorii de rețele publice de comunicații electronice asigură, cu prioritate, primirea și retransmiterea apelurilor către serviciul de urgență 112, indiferent dacă aceste apeluri sunt inițiate în rețeaua proprie sau în alte rețele publice de telefonie.*".

După cum menționează și respondentul în observațiile sale, obligația raportării acestui tip de incident este o noutate introdusă prin proiectul supus consultării, neexistând această obligativitate în cadrul normativ actual, însă dorim să atragem atenția că simpla notificare a Autorității cu privire la existența unui incident care a afectat rutarea comunicațiilor către Serviciul de urgență 112 nu presupune instituirea unor noi sarcini în vederea identificării acestor incidente, astfel că această obligație nu este incompatibilă cu protocoalele de comunicare directă existente între furnizori și STS. Suplimentar acestor protocoale pe care furnizorii le implementează deja, obligația de raportare a acestor incidente va permite Autorității să dețină o imagine de ansamblu clară asupra calității accesului la serviciile de urgență.

În concluzie, luând în considerare argumentele prezentate mai sus, considerăm că eliminarea subpunctului (i) nu ar fi în beneficiul general al industriei de comunicații electronice și nici al interesului public. Accesul la Serviciul de urgență 112 este vital pentru furnizarea de asistență rapidă în situații de urgentă, salvând vieți și contribuind la siguranța comunității. Ca urmare, ANCOM consideră extrem de importantă informarea acesteia cu privire la orice incident care afectează, pe o perioadă de cel puțin 15 minute, rutarea comunicațiilor de urgență către Serviciul de urgență 112, fără a impune, totodată, o obligație excesivă în sarcina furnizorilor, ținând cont și de termenul în care trebuie realizată notificarea inițială pe care furnizorii sunt obligați să o transmită ANCOM.

Având în vedere motivele expuse mai sus, Autoritatea respinge această observație.

În ceea ce privește **cel de-al doilea prag a cărui eliminare a fost solicitată de respondent, referitor la incidentele ce afectează furnizarea serviciilor de comunicații critice**, ANCOM notează faptul că, aceste servicii urmează a fi operaționalizate de către STS conform prevederilor Ordonanței de urgență a Guvernului nr. 73/2020[5], în baza unor acorduri semnate cu furnizorii de rețele și servicii publice mobile de comunicații electronice. Cu alte cuvinte, chiar dacă STS este furnizorul desemnat de servicii de comunicații critice, acestea vor fi afectate de incidente de securitate produse la nivelul rețelelor și serviciilor publice mobile de comunicații electronice, la momentul operaționalizării serviciilor de comunicații critice ANCOM urmând să reevalueze necesitatea impunerii unui astfel de prag în paralel cu dezvoltarea serviciilor de comunicații critice. Astfel, **ANCOM acceptă observația primită și elimină pragul calitativ**.

[4] Decizia președintelui ANCOM nr. 1023/2008 privind realizarea comunicațiilor de urgență către Sistemul naţional unic pentru apeluri de urgență, cu modificările și completările ulterioare.

[5] Ordonanța de urgență a Guvernului nr. 73/2020 privind desemnarea Serviciului de Telecomunicații Speciale ca integrator de servicii de comunicații critice, destinate autorităților publice cu atribuții în managementul situațiilor de urgență, aprobată prin Legea nr. 130/2022.

În legătură cu **cel de-al treilea element referitor la notificarea incidentelor care afectează operatorii de servicii esențiale**, respondentul a precizat că nu deține și nu poate deține informații cu privire la lista acestor operatori, neavând acces la Registrul Operatorilor de Servicii Esențiale (ROSE), care este un registru clasificat. **ANCOM acceptă această observație referitoare la eliminarea pragului prevăzut la subpct. (iv) al lit. b) de la pct. 5 alin. (1) al art. 2 din Proiect.**

Având în vedere cele menționate anterior, **dispozițiile art. 2 alin. (1) pct. 5 lit. b) din Proiect vor avea următorul conținut:**

„b) praguri calitative:

(i) incidente care afectează, direct sau indirect, pe o perioadă de cel puțin 15 minute, rutarea comunicațiilor de urgență către Serviciul de urgență 112;

(ii) incidente cu impact transfrontalier;

***(iii) incidente care afectează securitatea rețelelor și serviciilor altui furnizor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și îi cauzează acestuia un incident care are un impact semnificativ, în măsura în care această situație era cunoscută*."**

Totodată, dispozițiile relevante ale Anexelor nr. 2 și 3 la proiectul de decizie au fost revizuite corespunzător, prin eliminarea rubricilor aferente pragurilor eliminate.

2. Un respondent solicită eliminarea acelor „condiționări statistice" conținute în pragul cantitativ aferent proprietății de disponibilitate, considerând că valorile de 5.000 de utilizatori, timp de cel puțin 60 de minute sau pragul de 500.000 de „ore - utilizator" nu sunt utile în cazul persoanelor fizice, ținând cont de importanța oferirii către fiecare utilizator a unor servicii de calitate, care îndeplinesc fără nicio condiționare de prag cantitativ cele patru dimensiuni ale securității rețelelor și serviciilor. Aceleași observații referitoare la eliminarea pragului cantitativ au fost formulate şi referitor la pragul aferent celorlalte dimensiuni ale securității, respectiv, în cazul autenticității, integrității sau confidențialității, atunci când sunt afectați cel puțin 5.000 de utilizatori, indiferent de durata incidentului.

Răspunsul ANCOM:

Luând în considerare observația privind modificarea pragurilor cantitative pentru cele patru dimensiuni ale securității, reiterăm importanța menținerii pragurilor prevăzute de proiect și prezentăm câteva puncte suplimentare pentru a susține această poziție. În primul rând, stabilirea unor praguri cantitative în cazul incidentelor de securitate care au un impact semnificativ asigură că obligația de notificare se aplică evenimentelor care pot avea consecințe negative semnificative și evită o sarcină excesivă de notificare a incidentelor minore sau nesemnificative. Necesitatea stabilirii unor praguri rezultă, de altfel, chiar din dispozițiile art. 47 alin. (1) și (2) din Ordonanța de urgență a Guvernului nr. 111/2011, care stabilesc obligația furnizorilor de a notifica ANCOM acele incidente care au un impact semnificativ asupra rețelelor și serviciilor.

În al doilea rând, ANCOM a stabilit pragurile din cuprinsul proiectului în concordanță cu reglementările europene în vigoare, precum Codul European al Comunicațiilor Electronice (EECC), și/sau urmărind ghidurile emise de entități relevante, cum ar fi Agenția Europeană pentru Securitatea Cibernetică (ENISA). Aceste praguri au fost așadar concepute pentru a asigura coerența cu cerințele europene și pentru a se alinia la cele mai bune practici la nivel european în ceea ce privește gestionarea incidentelor în domeniul comunicațiilor electronice.

Astfel, în pofida preocupărilor exprimate, menținerea pragurilor cantitative actuale pentru disponibilitate și celelalte dimensiuni ale securității asigură un echilibru între obligația furnizorilor referitoare la notificarea ANCOM și obiectivul de asigurare a unei securități adecvate a rețelelor și serviciilor de comunicații electronice și, totodată, este conformă cu reglementările europene relevante transpuse, printre altele, și prin dispozițiile art. 47 alin. (1) și (2) din Ordonanța de urgență a Guvernului nr. 111/2011 menționate anterior.

Nu în ultimul rând, aducem la cunoștință faptul că, pentru evenimentele ce afectează calitatea şi/sau disponibilitatea serviciilor, la nivel de utilizator individual, se aplică prevederile legale referitoare la calitatea serviciilor, precum și la dreptul utilizatorilor serviciilor de comunicații electronice destinate publicului de a se adresa Autorității în cazul în care aceștia consideră că un furnizor nu își îndeplinește

obligațiile legale care intră în aria de competență a ANCOM. Conform atribuțiilor sale, Autoritatea a reglementat anumiți parametri de calitate a serviciului de acces la internet prin intermediul Deciziei președintelui ANCOM nr. 1112/2017[6].

Prin urmare, ANCOM nu poate accepta observația respondentului de eliminare a valorilor conținute de pragurile indicate de respondent.

3. Același respondent a solicitat mai multe completări ale proiectului de decizie, după cum urmează:

a. „Obligarea operatorilor de comunicatii de-a utiliza doar routere performante capabile sa informeze prompt, precis și complet operatorii cu privire la fluctuatiile si intreruperile conexiunii oricarui client la Internet". Totodată, respondentul solicită ca aceste echipamente să fie utilizate pentru efectuarea unor măsurători ale parametrilor conexiunii la internet;

b. „Obligarea operatorilor de comunicatii de-a masura exact si transparent - de preferinta si la client si la ei - duratele intreruperilor conexiunilor la Internet, in scopul acordarii unor despagubiri individuale, in anumite situatii.";

c. „Conditionarea acordarii anumitor facilitati/privilegii operatorilor de comunicatii de implementarea si certificarea periodica - in Romania si/ sau in Europa - unui sistem de management integrat - incluzand cel putin calitatea, securitatea informatiei, responsabilitatea sociala.";

d. „Obligarea operatorilor de comunicatii de-a solutiona prompt si eficace sesizarile clientilor lor (mai ales persoane fizice) privind intreruperile conexiunilor lor la Internet, inclusiv prin utilizarea metodelor si tehnicilor de telediagnostic si telementenanta (de ex. prin Team Viewer)".

Răspunsul ANCOM:

Cu privire la cele patru propuneri, Autoritatea învederează respondentului faptul că toate solicitările sale excedează domeniului de reglementare al acestui proiect de decizie, **astfel că acestea, precum și propunerile de completare, nu pot fi acceptate**.

4. Un respondent solicită revizuirea alin. (2) de la art. 5 din Proiect, în sensul modificării termenului de transmitere a notificării inițiale: de la *ora 13:00 a zilei <u>următoare</u> celei în care s-a petrecut incidentul,* la *ora 13:00 a zilei <u>lucrătoare următoare</u> celei în care s-a petrecut incidentul*. Solicitarea este motivată de faptul că obligația de a raporta incidentele şi în zilele nelucrătoare sau în cele de sărbători legale ar necesita resurse umane suplimentare din partea furnizorului, resurse ce ar putea fi utilizate pentru acțiuni de remediere sau intervenție pentru remedierea incidentelor. Notificarea incidentelor către ANCOM este văzută ca o activitate strict administrativă care nu ajută în vreun fel la remedierea situațiilor. Mai mult, respondentul își justifică solicitarea şi prin faptul că atribuțiile ANCOM nu prevăd implicarea în mod direct în rezolvarea problemelor, iar propunerea de modificare a termenului de raportare este disproporționată.

Legat de modificările aduse formularului de notificare prin Proiect, și mai precis de adăugarea câmpului legat de clasificarea incidentului notificat ca fiind unul repetitiv, respondentul a afirmat că informațiile sunt disponibile Autorității din istoricul raportărilor anterioare și că acest pas nu este necesar a fi impus furnizorilor. Prin urmare, se solicită eliminarea obligației de a preciza caracterul repetitiv al incidentului.

Răspunsul ANCOM:

Având în vedere argumentele aduse de respondent, precum și contextul în care se petrec incidentele în zilele considerate libere, ANCOM acceptă propunerea respondentului și modifică prevederea din Proiect, astfel încât termenul de trimitere a notificării inițiale va fi ora 13:00 a zilei <u>lucrătoare următoare</u> celei în care s-a petrecut incidentul. Cu toate acestea, pentru incidentele care afectează mai mult de 100.000 de utilizatori, se menține obligația de a raporta incidentul până la *ora 13:00 a zilei <u>calendaristice următoare</u> celei în care s-a petrecut incidentul*.

Instituirea pragului de 100.000 de utilizatori în zilele de sărbători legale sau în zilele considerate libere este justificat de faptul că un număr atât de mare de utilizatori afectați este posibil să devină un incident cu impact societal, caz în care este necesar ca și Autoritatea să fie înștiințată din timp

[6] Decizia președintelui ANCOM nr. 1112/2017 privind stabilirea indicatorilor de calitate pentru furnizarea serviciului de acces la internet și publicarea parametrilor aferenți, cu modificările și completările ulterioare.

astfel încât să poată să își exercite atribuțiile de supraveghere în mod adecvat, dacă este cazul. ANCOM reamintește că notificarea inițială, așa cum este prevăzută în Proiect, trebuie să conțină informații sumare despre incident, atfel că termenul mai scurt de transmitere a acesteia implică un efort suplimentar minim în procesul de raportare. Faptul că transmiterea notificării inițiale se realizează exclusiv prin intermediul e-mail-ului, fără necesitatea accesării vreunei aplicații informatice, ar trebui să contribuie la simplificarea procesului și la minimizarea impactului asupra resurselor necesare la nivelul furnizorilor de rețele și servicii publice de comunicații electronice.

Ca urmare, art. 5 alin. (2) din Proiect se va modifica și va avea următorul conținut:

(2) În aplicarea alin. (1), furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a transmite ANCOM o notificare inițială, până cel târziu la ora 13.00 a zilei lucrătoare următoare celei în care a fost detectat incidentul de securitate care are un impact semnificativ, cu excepția incidentelor care afectează mai mult de 100.000 utilizatori, care vor fi notificate până cel târziu la ora 13.00 a zilei calendaristice următoare celei în care a fost detectat incidentul.

Referitor la modificarea formularului de raportare prin adăugarea câmpului corespunzător caracterului repetitiv al incidentului, menționăm că furnizorii de rețele şi de servicii de comunicații electronice destinate publicului sunt cei mai în măsură să aprecieze caracterul repetitiv al incidentelor în propriile rețele. Menținerea acestui câmp în formularul de raportare aduce avantaje în ceea ce privește raportarea uniformă și analiza eficientă a incidentelor. Este o modalitate de a asigura consistența datelor raportate și de a ajuta Autoritatea să înțeleagă mai bine incidentele. Pe de altă parte, furnizorii ar trebui să fie în primul rând interesați de identificarea unui incident repetitiv pentru că astfel pot lua măsurile corective ce se impun pentru a întrerupe seria de incidente. Amintim că procesul de management al riscului și de stabilire a măsurilor de securitate adecvate se bazează și pe analiza incidentelor. Cu atât mai mult un incident repetitiv ar trebui să declanșeze o reacție în sensul îmbunătățirii măsurilor de securitate. Așadar, **considerăm că existența acestui câmp va aduce beneficii pentru ambele părți și, în consecință, câmpul aferent caracterului repetitiv al unui incident se va păstra în proiectul de decizie.**

II. Observații privind Grupul Consultativ pentru Securitatea Comunicațiilor Electronice

5. Un respondent solicită modificarea art. 8 alin. (3) din Proiect în sensul includerii asociațiilor de profil care reprezintă interesele furnizorilor de rețele publice de comunicații electronice care nu îndeplinesc criteriile privind numărul de conexiuni, în componența Grupului Consultativ pentru Securitatea Comunicațiilor Electronice, prevăzut la art. 8 alin. (1) din Proiect. Solicitarea este motivată de faptul că obligativitatea implementării măsurilor organizatorice și tehnice privind securitatea este impusă tuturor furnizorilor, indiferent de numărul de conexiuni.

Răspunsul ANCOM:

Astfel cum reiese și din conținutul art. 8 din Proiect și din expunerea de motive aferentă acestuia, Grupul Consultativ pentru Securitatea Comunicațiilor Electronice va fi constituit din reprezentanți ai ANCOM cu atribuții în securitatea rețelelor și serviciilor și din cel puțin un expert tehnic al fiecărui furnizor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului care au un număr de cel puțin 100.000 de conexiuni. În vederea creării unui cadru de cooperare în domeniul securității rețelelor și serviciilor de comunicații electronice, Grupul va asigura o comunicare mai facilă și rapidă între ANCOM şi furnizori pe diverse teme ce țin de domeniul securității rețelelor și serviciilor de comunicații electronice, identificarea unor soluții la probleme punctuale ce pot apărea, îmbunătățirea și promovarea continuă a securității rețelelor și serviciilor de comunicații electronice, diseminarea diverselor aspecte de securitate, inclusiv cele referitoare la incidente. Având în vedere importanța asigurării securității rețelelor și serviciilor de comunicații electronice, precum și amploarea pe care o pot avea anumite incidente, unele subiecte pot fi discutate cu precădere de către membrii grupului, în funcție de necesitățile sau de constrângerile identificate la momentul respectiv. Prin urmare, o restrângere a numărului de participanți poate fi necesară.

În cazul în care se vor dezbate subiecte care țin de aspecte generale referitoare la securitatea rețelelor și serviciilor de comunicații electronice, ANCOM poate invita la discuții și reprezentanții asociațiilor de profil care reprezintă interesele furnizorilor de rețele publice de comunicații electronice.

Pentru a încuraja și pentru a facilita colaborarea și cu alte entități, având în vedere că prevederile Proiectului se aplică tuturor furnizorilor, la art. 8 se va introduce un nou alineat cu următorul conținut: *(6) La întâlnirile Grupului prevăzut la alin. (1) vor putea fi invitați să participe și reprezentanți ai altor entități - autorități, instituții publice, persoane juridice de drept public sau privat și asociații de profil care reprezintă interesele furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului, care nu îndeplinesc criteriile de la alin. (3).*

III. Observații privind evaluarea securității rețelelor și serviciilor

6. Un respondent solicită completarea prevederilor art. 3 alin. (8) din Proiect în sensul definirii concrete a situației/cazurilor în care ANCOM poate solicita furnizorilor informațiile necesare evaluării securității. Totodată, se solicită și includerea unei metodologii care să permită identificarea modalității de evaluare a securității rețelelor și serviciilor de către ANCOM. Reamintim că forma actuală a textului prevede că: „*(8) Atunci când consideră necesar, ANCOM solicită furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului transmiterea, într-un termen stabilit de aceasta, dar care nu poate depăși 30 de zile de la primirea solicitării, a tuturor informațiilor necesare evaluării securității rețelelor și serviciilor, inclusiv a documentației ce a stat la baza implementării măsurilor de securitate, precum și a deciziei de excludere a anumitor obiective de securitate, în cazul furnizorilor prevăzuți la alin. (3)*."

Răspunsul ANCOM:

Obligația furnizorilor de a transmite, la solicitarea ANCOM, toate informațiile necesare evaluării securității rețelelor și serviciilor, inclusiv măsurile de securitate implementate și documentația ce a stat la baza acestora, este stabilită de prevederile art. 49 alin. (1) lit. a) din Ordonanța de urgență a Guvernului nr. 111/2011, după cum urmează: „*(1) În vederea aplicării prevederilor prezentului capitol, ANCOM poate solicita furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului: a) să furnizeze toate informațiile necesare evaluării securității rețelelor și serviciilor, inclusiv măsurile de securitate implementate și documentația ce a stat la baza acestora*.". Astfel cum se poate observa, legislația primară prevede explicit furnizarea tuturor informațiilor necesare evaluării securității rețelelor și serviciilor, inclusiv măsurile de securitate implementate și documentația ce a stat la baza acestora. Aceasta nu include limitări ale atribuțiilor ANCOM în ceea ce privește monitorizarea respectării obligațiilor furnizorilor (spre exemplu prin definirea concretă a situației/cazurilor în care ANCOM poate solicita furnizorilor informațiile necesare evaluării securității ori prin definirea unor modalități de evaluare a securității rețelelor și serviciilor de către ANCOM etc.). Completarea prevederilor art. 3 alin. (8) din Proiect în conformitate cu solicitarea respondentului ar reprezenta o limitare a atribuțiilor Autorității. Art. 3 alin. (8) din Proiect are rolul de a stabili un termen clar de transmitere a informațiilor necesare prevăzute de dispozițiile legale citate anterior.

Mai mult, așa cum s-a menționat și în cap. *6. Domeniile și obiectivele de securitate aferente acestora* din expunerea de motive, furnizorii au obligația de a lua toate măsurile tehnice și organizatorice adecvate, obiective și proporționale pentru a gestiona în mod corespunzător riscurile la adresa securității rețelelor și serviciilor de comunicații electronice. Măsurile luate trebuie să asigure un nivel de securitate corespunzător riscului identificat. Prin urmare, într-o primă etapă, furnizorii trebuie să efectueze analize specifice pentru situația lor particulară, pentru a determina ce resurse se află în domeniul de aplicare, iar, ulterior, să efectueze o evaluare a riscurilor pentru a determina măsurile de securitate adecvate. În acest sens, pentru a veni în sprijinul furnizorilor în ceea ce privește implementarea acestor prevederi, în expunerea de motive au fost menționate câteva standarde și ghiduri relevante care conțin descrieri inclusiv referitoare la modalitățile de evaluare a securității.

Prin urmare, la solicitarea ANCOM, furnizorii vor pune la dispoziția Autorității informațiile și documentele relevante utilizate în procesul de realizare a analizei de risc, de identificare și de implementare a măsurilor de securitate implementate.

Având în vedere motivele expuse mai sus, Autoritatea respinge această observație.

IV. Observații privind obligația de a asigura back-up electric

7. Un respondent solicită introducerea noțiunii de „back-up electric mobil", și, astfel, și a obligației furnizorilor de a asigura o astfel de facilitate, ca o soluție sau o combinație de soluții tehnice de alimentare cu energie electrică, mobile, ce urmează a fi instalate într-o locație care găzduiește echipamente de rețea de comunicații electronice, având rolul de asigurare a continuității în funcționarea echipamentelor de rețea, respectiv a serviciilor oferite utilizatorilor prin intermediul echipamentelor respective, cu capabilitate de back-up de minimum 24 ore în caz de întrerupere a alimentării cu energie electrică din rețeaua de distribuție și cu un timp impus operatorilor în vederea instalării si operaționalizării unor astfel de soluții de maximum 6 ore, pentru unitățile centrale de comutație/control și hub-urile de transmisiuni.

Răspunsul ANCOM:

ANCOM înțelege necesitățile de reziliență în alimentarea cu energie electrică necesare, în special în suportul comunicațiilor de urgență. Analizând măsura propusă, Autoritatea consideră însă că aceasta nu va conduce în mod implicit la îmbunătățirea semnificativă a indicilor de disponibilitate a echipamentelor hardware componente ale rețelelor de comunicații electronice, întrucât o bună parte din elementele care concentrează fluxuri majore de trafic (de exemplu, centrale, hub-uri mari de transmisiuni) sunt deja securizate în acest sens, în principal cu generatoare fixe sau generatoare fixe plus acumulatori. Din punct de vedere practic, de asemenea, utilizarea unor generatoare mobile pentru a asigura astfel de durate de back-up ar necesita măsuri logistice nespecifice unor astfel de soluții (de exemplu, supradimensionarea/realimentarea rezervoarelor cu combustibil).

Totodată, Autoritatea notează că back-up-ul electric mobil este o soluție versatilă, pretabilă în mod optim alocării dinamice, în funcție de necesitățile apărute, cu mecanism logistic propriu. În acest sens, ar putea fi luată în considerare înființarea unui pool național de resurse de back-up, cu implicarea părților interesate. Acest aspect a fost deja discutat cu participarea operatorilor de comunicații și asumat ca un deziderat important la nivel național pentru îmbunătățirea securității comunicațiilor publice mobile, în cadrul ședinței unui grup de lucru interinstituțional care a dezbătut subiectul rezilienței comunicațiilor electronice.

Prin urmare, având în vedere cele menționate anterior, ANCOM respinge propunerea respondentului referitoare la noțiunea de back-up electric mobil și la introducerea unor obligații corespunzătoare în sarcina furnizorilor.

8. Un respondent solicită eliminarea art. 4 din Proiect referitor la obligația de a asigura valori minime ale duratelor de back-up electric fix, cu precădere din perspectiva comunicațiilor mobile, pe cinci direcții de argumentație:

a) trendul descendent indicat de rapoartele anuale ale ANCOM, atât în ceea ce privește numărul incidentelor cu impact semnificativ, cât și în ceea ce privește numărul incidentelor generate de lipsa alimentării cu energie electrică, evidențiat în cazul incidentelor cu impact semnificativ;

b) lipsa cadrului legislativ care să impună la nivel european astfel de obligații, precum și existența unor măsuri similare la nivelul Uniunii Europene în doar 2 țări (Suedia și Finlanda), amintite de ANCOM în studiul publicat în luna martie 2021 privind incidentele de securitate provocate de întreruperea furnizării energiei electrice;

c) oportunitatea tratării cauzelor și nu a efectelor întreruperilor cu energie electrică asupra rețelelor și serviciilor de comunicații electronice (prin protocoale de colaborare între ANCOM și Autoritatea Națională de Reglementare în domeniul Energiei (ANRE), care să prioritizeze restabilirea alimentării cu energie pentru locațiile în care există elemente de rețea importante pentru furnizarea serviciilor de comunicații electronice), implicarea statului ca factor de susținere în continuitatea

furnizării serviciilor (din perspectivă economică și pentru diminuarea unor constrângeri aplicabile în zona telecom pentru a contracara problemele din domeniul energetic);

d) constrângeri de ordin fizic/spațiu necesar echipamentelor adiționale și securitatea asociată acestora;

e) costurile adiționale generate de măsură, care se adaugă celor determinate de aplicarea Legii nr. 163/2021[7], cheltuielile generate de licitația recentă de spectru/condițiile licențiate, restricțiile legate de amprenta de carbon și costurile de reciclare a acumulatorilor.

În schimb, același respondent își exprimă disponibilitatea de a purta viitoare discuții pe tema incidentelor care au drept cauză lipsa alimentării cu energie electrică, prin intermediul grupului consultativ prevăzut de art. 8 din Proiect, în scopul identificării unor soluții care să minimizeze apariția acestui tip de incidente.

Răspunsul ANCOM:

În ceea ce privește solicitarea de eliminare a art. 4 din textul proiectului de decizie, considerăm că, în contextul trecerii către o societate tot mai digitalizată și al dependenței tot mai crescute a activităților de zi cu zi – fie că vorbim de interacțiunea cu administrația publică, comerțul cu bunuri și servicii, munca de la distanță în domenii tot mai variate și mai numeroase, divertismentul online și on demand – buna funcționare a rețelelor publice de comunicații electronice, îndeosebi a rețelelor de comunicații mobile, este o condiție *sine qua non* pentru realizarea tuturor acestor activități. Astfel, măsurile de asigurare a continuității furnizării serviciilor de comunicații devin tot mai importante pentru toate categoriile de utilizatori, întreruperi ale furnizării acestor servicii întinse pe durate de ordinul orelor devenind tot mai puțin acceptabile.

Din perspectiva incidentelor de securitate care au un impact semnificativ raportate de operatori, ANCOM precizează că numărul acestor incidente având drept cauză lipsa alimentării cu energie electrică raportate anual se menține la nivelul sutelor de incidente, aceasta fiind de departe cauza cea mai importantă de producere a incidentelor semnificative raportate. Astfel, conform *Raportului*[8] *privind incidentele care au afectat securitatea rețelelor și serviciilor de comunicații electronice în anul 2022*, disponibil pe site-ul ANCOM, se observă un trend ușor ascendent al incidentelor cauzate de discontinuități în furnizarea energiei electrice, cu un maxim local/anual de 55%, potrivit graficului următor (Figura 1). Totodată, reținem că durata medie a incidentelor cu cauza menționată se situează în jurul valorii de 6 ore, cu un maxim absolut al duratei medii de 6 ore și 28 minute, înregistrat în 2022 (Figura 2).

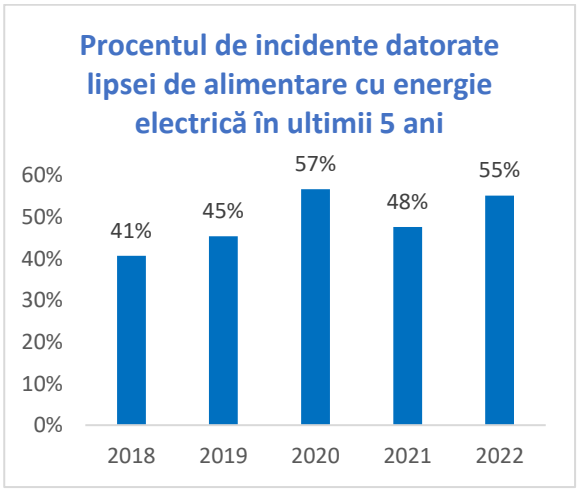

Figura 1

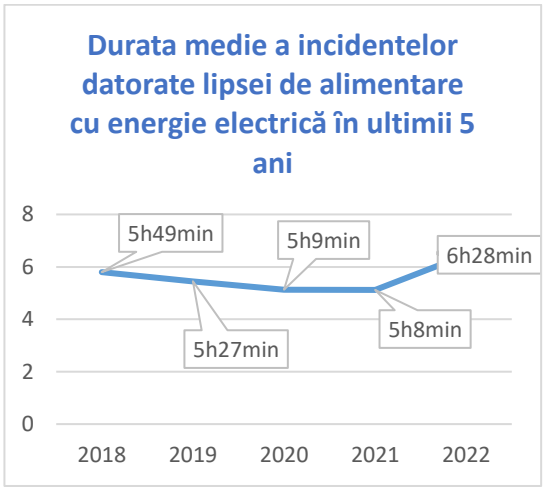

Figura 2

Totodată, precizăm că scopul elaborării Art. 4 din Proiect, respectiv introducerea unor durate reglementate de back-up electric, îl reprezintă inclusiv adresarea problemelor de disponibilitate și de asigurare a continuității serviciilor care nu se regăsesc în categoria incidentelor cu impact semnificativ,

[7] Legea nr. 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice şi de comunicaţii de interes naţional şi condiţiile implementării reţelelor 5G.

[8] https://www.ancom.ro/uploads/links_files/ANCOM_Raport_incidente_2022_iulie_2023.pdf

adică cele raportabile imediat Autorității, dar care și ele afectează funcționarea anumitor elemente de rețea. În vreme ce incidentele cu impact semnificativ, care afectează rețelele de comunicații mobile, sunt de ordinul câtorva sute anual, celelalte incidente care afectează tronsoane de rețea (radio, în principal) sunt de până la 100.000/an, potrivit studiului publicat de ANCOM în anul 2021, pe baza datelor colectate de la operatori[9]. Nu în ultimul rând, ANCOM remarcă faptul că în raport cu datele transmise de furnizori cu privire la back-up-ul deja existent/instalat, duratele propuse spre a fi impuse prin reglementare nu ar trebui să ridice probleme deosebite, cea mai mare parte dintre locații/elemente de rețea fiind raportate ca beneficiind deja de sisteme de back-up electric cu durate sensibil echivalente cu cele stabilite prin propunerea de reglementare. Astfel, scopul primordial al reglementării îl constituie tocmai sistematizarea și permanentizarea măsurilor rezonabile de back-up electric utilizate deja de furnizorii de rețele publice de comunicații electronice.

Preocupările în sensul creșterii rezilienței sectorului de comunicații, ca pilon al societății informaționale contemporane și ca bază a rezilienței unui stat în ansamblul său se situează la cote ridicate la nivel internațional. România trebuie să adopte măsurile specifice/adecvate dinamicii și particularităților mediului local, în acest sens avându-se în vedere nivelul calitativ al furnizării energiei electrice în rețeaua națională din România, dar și caracteristicile geografice/de relief specifice, cu implicații directe în timpii de acces la echipamentele de comunicații situate în locații greu accesibile. Opinăm că aceste particularități reprezintă un argument în a ne afla în primul eșalon de țări care adoptă în mod explicit astfel de măsuri, cu atât mai mult cu cât – subliniem – duratele de back-up electric impuse nu reprezintă un impediment în respectarea obligației de către furnizorii vizați de aceasta.

În ceea ce privește implicarea/cooperarea între părțile interesate din domeniul comunicațiilor electronice și cele din domeniul energiei, precizăm că acesta este un deziderat aflat printre măsurile identificate pentru sporirea rezilienței comunicațiilor publice, colaborarea între autorități și între furnizorii de comunicații și distribuitorii de energie este o măsură complementară obligațiilor impuse furnizorilor de comunicații, ambele tipuri de măsuri adresând în mod corespunzător, pe paliere diferite, problematica discontinuităților în alimentarea cu energie electrică. Nu se dorește, așadar, exercitarea unei presiuni suplimentare asupra celor implicați în domeniul comunicațiilor în favoarea actorilor din energie, Proiectul propunându-și inclusiv o detaliere a măsurilor pe care furnizorii au obligația de a le lua pentru a asigura o securitate adecvată a utilităţilor suport, acesta constituind doar unul dintre obiectivele de securitate care trebuie atinse de furnizori în vederea asigurării securității rețelelor și serviciilor de coomunicații electronice.

ANCOM a inițiat totodată prime discuții cu ANRE în scopul identificării celor mai bune soluții pentru problemele cu care se confruntă furnizorii de rețele publice de comunicații electronice și a unor modalități optime de colaborare între cele două autorități în vederea minimizării timpilor de întrerupere a furnizării de energie electrică, inclusiv în vederea facilitării unei comunicări mai strânse între operatorii de distribuție de energie electrică și furnizorii de comunicații electronice.

În ceea ce privește constrângerile de ordin fizic, precizăm că asigurarea securității elementelor de rețea, indiferent de natura sau de tipul lor, constituie o obligație deja în vigoare și are chiar un caracter implicit evident din punct de vedere tehnic. ANCOM notează că reglementarea în discuție nu vizează introducerea soluțiilor de back-up electric fix în rețelele de comunicații, ca element nou, asociat acestora. Constrângerile legate de spațiu, de asemenea, sunt aplicabile și altor elemente, ca de exemplu celor care fac obiectul unui upgrade de capacitate (RRU, BBU, sisteme radiante etc.) și pot fi gestionate punctual.

Având în vedere datele raportate în cadrul chestionarului ANCOM din anul 2020 de către operatori cu privire la back-up-ul existent, rezultă că impactul financiar generat de introducerea dispozițiilor art. 4 din Proiect nu este unul împovărător. Impactul financiar nu ar trebui privit de sine stătător ca un element singular, Autoritatea considerând că beneficiile aduse de implementarea măsurilor de back-up contrabalansează eventualele dezavantaje de ordin economic. Toate aceste

[9] https://www.ancom.ro/uploads/links_files/Incidente_energie_studiu_2021.pdf

aspecte au fost luate în considerare de Autoritate la stabilirea duratei de implementare la nivel de rețea.

Pentru a veni în întâmpinarea doleanțelor respondenților, ANCOM înțelege să circumstanțieze obligația privind valorile minime ale duratelor de back-up electric fix, după cum urmează:

- introducerea definiției *hub-ului de transmisiuni* considerat a fi locația care concentrează traficul generat de cel puțin 8 elemente de rețea (de ex., site-uri radio), **prevederile art. 2 alin. (1) din Proiect completându-se, astfel, cu un pct. 8, având următorul conținut: *„8. hub de transmisiuni - un element de rețea care concentrează traficul generat de cel puțin alte 8 elemente de rețea (de ex., site-uri radio)*."**
- în municipiile reședință de județ, potrivit art. 4 alin. (1) lit. a), se stabilește o durată minimă de back-up electric fix standard de o oră pentru orice element de rețea, întrucât s-au luat în calcul atât densitatea elementelor de rețea/overlapping, termenele mai mici de restabilire în caz de incident energetic, la nivelul furnizorilor de energie, dar și accesul mai facil al echipelor de teren care să suplinească, după caz, necesarul energetic prin soluții de back-up mobil (generatoare);
- menținerea, în cuprinsul art. 4 alin. (1) lit. b) din Proiect, a duratei minime de back-up electric fix standard de 3 ore pentru orice element de rețea situat în afara municipiilor reședință de județ, ca urmare a modificărilor efectuate literei a) menționate anterior;
- excluderea din calculul necesarului de back-up a echipamentelor de climatizare pentru categoriile reglementate de art. 4 alin. (1) lit. a) și lit. b) din Proiect, furnizorii având însă obligația să asigure regimul termic/condițiile tehnice adecvate de funcționare a echipamentelor pe toată durata alimentării din sursa de back-up.
- exceptarea de la obligația de a avea soluții de back-up electric pentru echipamentele de rețea fixă aflate în proximitatea locațiilor utilizatorilor finali, precum acele cabinete stradale sau camerele tehnice telecom ale clădirilor, care găzduiesc echipamente de comunicații ce preced echipamentele terminale (CPE[10]), întrucât CPE ale abonatului ar fi oricum nefuncționale în eventualitatea apariției unui incident electric în zonă, cu excepția cazului în care utilizatorul și-ar fi asigurat singur o soluție de back-up electric pentru aceste echipamente.

Pentru toate aceste considerente, art. 4 se va revizui, după cum urmează:

*„**Art. 4.** – (1) În vederea creșterii nivelului de securitate a rețelelor și serviciilor de comunicații electronice, furnizorii de rețele publice de comunicații electronice care au un număr de cel puțin 100.000 de conexiuni sau care au rețele amplasate pe teritoriul a cel puțin 100 de unități administrativ-teritoriale de bază, din cel puțin 20 de județe, au obligația de a respecta următoarele valori minime ale duratelor de back-up electric fix:*

a) o oră – timp de back-up electric fix standard, durată aplicabilă oricărui element de rețea situat în municipiile reședință de județ;

b) 3 ore – timp de back-up electric fix standard, durată aplicabilă oricărui element de rețea situat în afara municipiilor reședință de județ;

c) 6 ore – timp de back-up electric fix extins, durată aplicabilă următoarelor elemente de rețea: unități centrale de comutație/control, hub-uri de transmisiuni, elemente de rețea din locații cu acces fizic dificil și locații identificate statistic ca având incidență sau frecvență de apariție a avariilor electrice ridicate.

(2) Capacitatea de back-up electric necesară în vederea respectării valorilor de la alin. (1) se va calcula avându-se în vedere puterea maximă absorbită de echipamentul de securizat, așa cum este aceasta marcată pe echipament sau declarată de producătorul acestuia.

(3) În calculul capacității de back-up electric necesară în vederea respectării valorilor de la alin. (1) se va avea în vedere și puterea maximă absorbită de sistemele de climatizare, sistemele de supraveghere alarme externe și sistemele de control-acces.

(4) Prin excepție de la prevederile alin. (3), în calculul capacității de back-up electric necesară în vederea respectării valorilor de la alin. (1) lit. a) și b) nu se va avea în vedere puterea maximă absorbită de sistemele de climatizare.

[10] CPE semnifică Customer Premises Equipment

(5) Sunt exceptate de la prevederile alin. (1) lit. a) și b) echipamentele de acces radio din categoriile repetoarelor instalate în interiorul clădirilor, a microcelulelor, precum și echipamentele de rețea fixă instalate în locațiile utilizatorilor finali sau în proximitatea locațiilor utilizatorilor finali.

(6) Dispozițiile alin. (5) nu se aplică echipamentelor care oferă servicii specifice tehnologiei mobile aferente rețelelor definite potrivit dispozițiilor art. 2 lit. f) din Legea nr. 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice şi de comunicaţii de interes naţional şi condițiile implementării rețelelor 5G, respectiv URLLC și mMTC.

(7) Furnizorii de rețele publice de comunicații electronice prevăzuți la alin. (1) vor transmite în format electronic către ANCOM până la data de 10 februarie a fiecărui an, lista privind locațiile încadrabile la data de 31 decembrie anul anterior în categoria specificată la alin. (1) lit. c).

(8) Prima raportare în conformitate cu alin. (7) se va realiza până la data de 10 februarie 2025."

Suplimentar, pentru a permite furnizorilor realizarea unei analize și a elaborării adecvate a tuturor soluțiilor tehnice necesare pentru implementarea noilor prevederi, în condiții de înaltă calitate tehnică, precum și de a permite realizarea procedurilor de achiziție a soluțiilor de back-up electric, ANCOM extinde perioada de implementare a acestei obligații, de la 1 an, la 18 luni.

Pentru acest considerent, art. 11 se va revizui astfel:

„Art. 11. *– (1) Prezenta decizie se publică în Monitorul Oficial al României, Partea I și intră în vigoare la data publicării, cu excepția prevederilor art. 3 care intră în vigoare în termen de 3 luni de la data publicării prezentei decizii în Monitorul Oficial al României, Partea I și a prevederilor art. 4 care intră în vigoare în termen de 18 luni de la data publicării prezentei decizii în Monitorul Oficial al României, Partea I."*

Totodată, ANCOM ia notă de disponibilitatea respondentului de a aborda, în cadrul grupului consultativ prevăzut de art. 8 din Proiect, tema incidentelor care au drept cauză lipsa alimentării cu energie electrică, în scopul identificării unor soluții care să minimizeze apariția acestui tip de incidente.

V. Observații privind măsurile de securitate specifice rețelelor 5G

9. Un respondent solicită eliminarea cerințelor de securitate din Anexa nr. 1 la Proiect care stabilesc măsuri specifice de securitate aplicabile exclusiv rețelelor definite prin dispozițiile art. 2 lit. f) din Legea nr. 163/2021. Respondentul consideră că Legea nr. 163/2021 stabilește un regim juridic special aplicabil utilizării tehnologiilor, echipamentelor și programelor software în cadrul rețelelor 5G, impunând autorizarea producătorilor de astfel de tehnologii, echipamente și programe software, bazată pe o evaluare a riscurilor, amenințărilor și vulnerabilităților la adresa securității naționale și apărării țării. Ca urmare, în opinia respondentului, nu ar fi necesară stabilirea, prin Proiect, în sarcina furnizorilor a unor obligații legate de luarea unor măsuri de securitate specifice rețelelor 5G, impunerea unor obligații specifice suplimentare în legătură cu rețelele 5G fiind o abordare excesivă și disproporționată, respondentul susținând că prin procedura de autorizare a producătorilor ar fi asigurate deja cerințele specifice de securitate aplicabile rețelelor 5G.

Răspunsul ANCOM:

Prin adoptarea Legii nr. 163/2021, s-a urmărit, în scopul prevenirii, contracarării şi eliminării riscurilor, ameninţărilor şi vulnerabilităţilor la adresa securităţii naţionale şi apărării ţării, adoptarea unui set de măsuri referitoare la autorizarea producătorilor de tehnologii, echipamente şi programe software utilizate în cadrul infrastructurilor informatice şi de comunicaţii de interes naţional, precum şi în reţelele de comunicaţii electronice prin intermediul cărora se asigură servicii de comunicaţii electronice de tip 5G. Acest segment este relevant întrucât modul în care sunt proiectate să funcționeze tehnologiile, echipamentele și programele software are impact direct asupra securității rețelelor și serviciilor de comunicații electronice și, implicit, asupra domeniilor securității naționale și de apărare a țării. Legea nr. 163/2021 a avut în vedere evaluările de risc la nivel național, precum și

pe cele la nivel european și prevederile Setului[11] de instrumente al Uniunii Europene privind securitatea cibernetică a rețelelor 5G (Setul de instrumente 5G). În principal, Legea are în vedere analizarea unor situații obiective în care s-ar putea afla producătorii de tehnologii, echipamente și programe software utilizate în cadrul rețelelor 5G, precum: lipsa unei structuri transparente a acționariatului producătorului, lipsa unei conduite etice a producătorului, funcționarea producătorului într-un sistem juridic care nu impune practici corporative transparente. Aceste elemente ce se pot concretiza într-un risc la adresa securității naționale sunt doar o parte dintre cele care sunt avute în vedere în procesul de analizare a cererilor de autorizare, existând multiple alte riscuri identificate în raportul[12] de evaluare coordonată la nivelul UE a riscurilor legate de securitatea rețelelor 5G. În baza acestui raport, Setul de instrumente 5G a inclus o serie de măsuri de securitate care urmăresc atenuarea eficace a riscurilor și asigurarea securității rețelelor 5G instalate în Europa. Acesta stabilește planuri de atenuare detaliate pentru fiecare risc identificat și stabilește o serie de măsuri strategice și tehnice esențiale, care ar trebui luate de toate statele membre și/sau de Comisie.

Includerea unor obiective de securitate specifice rețelelor 5G în Proiect a fost determinată de măsurile tehnice prezente în Setul de instrumente 5G: asigurarea aplicării cerințelor de securitate de bază (arhitectură și proiectare rețea sigure), implementarea măsurilor de securitate din standardele 5G și evaluarea acestei implementări, asigurarea unor măsuri de acces stricte, creșterea securității funcțiilor de rețea virtualizate, asigurarea unor procese de management, operațiuni și monitorizare a rețelei 5G sigure, consolidarea securității fizice, consolidarea integrității software-ului, a securității actualizărilor și a gestionării corecțiilor, ridicarea standardelor de securitate a produselor producătorilor prin condiții robuste de achiziții, consolidarea rezilienței și a planurilor de continuitate. Implementarea Setului de instrumente 5G este o prioritate pentru Comisia Europeană, iar statele membre ar trebui să instituie măsuri și să dispună de competențe pentru a atenua riscurile identificate. Acestea ar trebui, în special, să întărească cerințele de securitate pentru operatorii rețelelor mobile. În comunicarea sa din 15 iunie 2023, Comisia a luat act de adoptarea celui de-al doilea raport intermediar cu privire la punerea în aplicare a Setului de Instrumente 5G de către Grupul de cooperare NIS și a precizat că Statele Membre ar trebui să pună în aplicare fără întârziere setul de instrumente. De asemenea, Statelor Membre li se recomandă să utilizeze 5G Security Controls Matrix[13] elaborată de ENISA ca instrument de sprijinire a punerii în aplicare a măsurilor tehnice. Această matrice conține măsurile de securitate din ghidurile ENISA Guideline on Security Measures under the EECC[14] și 5G Supplement[15]. Primul ghid conține măsuri generale de securitate, ce țin de implementarea prevederilor art. 40 – 41 din Codul european al comunicațiilor electronice[16], în mod independent de serviciile furnizate sau de tipul rețelelor de comunicații electronice. Suplimentul 5G vine în completarea ghidului menționat anterior și conține măsuri specifice rețelelor 5G. Matricea 5G conține pe lângă măsurile de securitate de nivel înalt din cele două ghiduri și controale tehnice din standarde, bune practici din industrie și specificații tehnice, inclusiv specificațiile 3GPP. Matricea a fost consultată cu industria, ENISA colectând feedback cu privire la aceasta de la experții care își desfășoară activitatea în cadrul operatorilor de comunicații electronice din Uniune. ANCOM a informat operatorii de comunicații mobile din România cu privire la procesul de consultare publică și i-a invitat să facă observații și comentarii.

Proiectul urmărește astfel implementarea în legislația națională a măsurilor tehnice cuprinse în Setul de Instrumente 5G și apoi detaliate în 5G Supplement to the Guideline on Security Measures under the EECC. Scopul introducerii obiectivelor de securitate specifice rețelelor 5G îl constituie crearea unui cadru clar, uniform și predictiv în ceea ce privește măsurile pe care trebuie să le ia operatorii în vederea asigurării securității rețelelor și serviciilor. Acest lucru este cu atât mai important cu cât Setul de Instrumente 5G cere ca autoritățile competente să verifice, inclusiv prin audituri, măsurile implementate de furnizorii de rețele mobile și să ceară acestora să documenteze și să păstreze o descriere a modului de implementare a măsurilor tehnice de securitate. Cu alte cuvinte, reglementarea prezentată în cadrul proiectului nu are scopul de a dubla reglementarea existentă la nivel primar, prin Legea nr. 163/2021, ci vine în completarea acesteia. Legea nr. 163/2021 se adresează în special

[11] https://ec.europa.eu/commission/presscorner/detail/ro/ip_20_123
[12] https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security
[13] https://www.enisa.europa.eu/publications/5g-security-controls-matrix
[14] https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc/
[15] https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc
[16] Transpuse în legislația națională prin dispozițiile Capitolului IV: Securitatea rețelelor și serviciilor de comunicații electronice din Ordonanța de urgență a Guvernului nr. 111/2011.

producătorilor de tehnologii, echipamente și programe software utilizate în cadrul rețelelor 5G și în subsidiar furnizorilor de rețele și servicii de comunicații electronice (prin interzicerea săvârșirii faptelor prevăzute la art. 13), pe când proiectul de decizie al ANCOM se adresează în mod direct furnizorilor de rețele publice de comunicații electronice și de servicii de comunicații electronice destinate publicului, având drept scop asigurarea securității rețelelor 5G și a serviciilor oferite prin intermediul acestora, prin adoptarea de măsuri specifice la nivelul furnizorilor și a rețelelor acestora, acționând pe paliere diferite față de Legea nr. 163/2021.

În final, subliniem importanța menținerii unor măsuri de securitate specifice rețelelor 5G având în vedere dezvoltarea preconizată a acestora, precum și importanța lor pentru asigurarea unor servicii de tipul IoT, M2M, smart cities, cu un grad de securitate corespunzător.

Prin urmare, ANCOM respinge propunerea respondentului referitoare la eliminarea cerințelor de securitate din Anexa nr. 1 la Proiect care stabilesc măsuri specifice rețelelor definite prin dispozițiile art. 2 lit. f) din Legea nr. 163/2021.

10. Doi respondenți solicită definirea noțiunilor de „*funcții critice*" și „*zone critice*" astfel încât măsurile de securitate suplimentare specifice rețelelor definite prin dispozițiile art. 2 lit. f) din Legea nr. 163/2021, precum și orice proceduri de autorizare prevăzute în legislația privind securitatea rețelelor să se aplice doar funcțiilor de rețea critice și zonelor critice ale acestor rețele. Respondenții justifică solicitarea prin trimiterea la *Analiza de Risc privind Securitatea Cibernetică a Rețelelor 5G* și la *Setul de Instrumente privind Securitatea Cibernetică a Rețelelor 5G* care utilizează noțiunea de „elemente/funcții de rețea cheie (*key assets*)" pentru a diferenția elementele de rețea 5G în funcție de importanța acestora, clasificând nivelurile acestora de senzitivitate în funcție de natura și dimensiunea impactului unui incident de securitate asupra acestor funcții/elemente de rețea. Totodată, respondenții înțeleg că există anumite amplasamente strategice din perspectiva siguranței și apărării naționale care vor necesita implementarea unor măsuri de securitate mai severe.

Răspunsul ANCOM:

În ceea ce privește introducerea noțiunilor de „funcții critice" și „zone critice", ANCOM precizează că acestea au fost tratate în *Raportul privind evaluarea coordonată la nivelul UE a riscurilor în materie de securitate cibernetică aferente rețelelor de a cincea generație (5G)*[17]. Acest raport analizează diferiți actori care pot genera amenințări, sensibilitatea principalelor resurse ale rețelei, vulnerabilitățile legate de hardware, software, procese și politici și, în baza acestor 3 elemente, raportul identifică nouă riscuri principale grupate în cinci scenarii de risc. Pornind de la aceste riscuri, *Setul de Instrumente 5G* identifică o serie de măsuri strategice, măsuri tehnice și acțiuni de suport în vederea susținerii implementării măsurilor. Scopul acestora este de a reduce riscurile identificate și de a asigura securitatea rețelelor 5G. Așa cum se poate observa, sensibilitatea resurselor a fost tratată în cadrul documentelor precizate mai sus, iar măsurile identificate în cadrul *Setului de instrumente 5G* țin cont de aceste elemente. Măsurile din proiectul de decizie se bazează pe măsurile identificate în *Setul de instrumente 5G*. O abordare bazată pe riscurile identificate, asociată cu măsurile necesare pentru eliminarea sau atenuarea acestora, a stat și la baza elaborării Proiectului, ANCOM stabilind, astfel, pe baza documentelor menționate anterior, un set de măsuri pe care furnizorii sunt obligați să le implementeze în scopul asigurării securității rețelelor și serviciilor de comunicații electronice.

În ceea ce privește limitarea procedurii de autorizare prevăzută de Legea nr. 163/2021 printr-o decizie a ANCOM astfel încât procedurile de autorizare reglementate de Legea nr. 163/2021 să se aplice doar funcțiilor de rețea critice și zonelor critice ale rețelelor, precizăm că aceasta nu este posibilă din punct de vedere legal, o decizie neputând modifica prevederile unei legi. Suplimentar, așa cum am menționat și la punctul precedent, obiectivele urmărite de cele două acte sunt diferite. Scopul Legii nr. 163/2021 este adoptarea unor măsuri referitoare la autorizarea producătorilor de tehnologii, echipamente și programe software (utilizate în cadrul infrastructurilor informatice și de comunicații de interes național, precum și în rețelele de comunicații electronice prin intermediul cărora se asigură servicii de comunicații electronice de tip 5G) în vederea prevenirii, contracarării și eliminării riscurilor,

[17] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

amenințărilor și vulnerabilităților la adresa securității naționale și apărării țării. În cazul proiectului ANCOM, scopul este stabilirea măsurilor tehnice și organizatorice care trebuie luate de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului pentru a gestiona în mod corespunzător riscurile la adresa securității rețelelor și serviciilor de comunicații electronice, în baza prevederilor art. 46 alin. (1) și (2) din Ordonanța de urgență a Guvernului nr. 111/2011, precum și a *Setului de instrumente 5G*. Măsurile luate de furnizori pentru a îndeplini obiectivele de securitate precizate în decizie trebuie să asigure un nivel de securitate corespunzător riscului identificat, ținând seama de stadiul actual al tehnologiei și să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor și asupra altor rețele și servicii. Așadar, într-o primă etapă, furnizorii trebuie să efectueze analize specifice pentru situația lor particulară, pentru a determina ce resurse se află în domeniul de aplicare, iar, ulterior, să efectueze o evaluare a riscurilor pentru a determina măsurile de securitate adecvate. Evaluările riscurilor se vor actualiza periodic pentru a adresa și eventualele modificări efectuate asupra rețelei, precum și incidentele de securitate înregistrate.

Prin urmare, având în vedere cele sus-menționate, ANCOM nu consideră necesară realizarea unei distincții în cuprinsul Proiectului între funcții/zone critice și restul funcțiilor sau zonelor dintr-o rețea și, astfel, definirea unor criterii sau noțiuni care să susțină această distincție.

VI. Observații privind Anexa nr. 1 - Domeniile vizate de măsurile de securitate

11. Un respondent solicită introducerea în cadrul Anexei nr. 1 la Proiect a mai multor obligații ce vizează comunicațiile de urgență, având în vedere prevederile din expunerea de motive cu privire la statisticile referitoare la numărul incidentelor electrice, precum și impactul acestora asupra continuității furnizării accesului la Serviciul de urgență 112. Pentru furnizarea cu prioritate a comunicațiilor de urgență care să permită accesul permanent al cetățenilor la Serviciul de urgență 112, respondentul consideră necesară reglementarea unor măsuri suplimentare, atât pe linia continuității serviciului, cât și pe cea a restabilirii cu prioritate a acestuia. Solicitarea vizează următoarele:

- completarea *Domeniului IV. Managementul operaţiunilor* din Anexa nr. 1 la Proiect cu un nou punct, punctul 6) cu următorul conținut: „*6) să efectueze evaluări prealabile ale impactului potențial al unei schimbări de sistem.*"
- completarea *Domeniului V. Managementul incidentelor* din Anexa nr. 1 la Proiect cu un nou punct, punctul 6) cu următorul conținut: „*6) să stabilească proceduri și procese pentru restabilirea prioritară a serviciilor ce asigură comunicațiile de urgență.*"
- completarea *Domeniului VI. Managementul continuităţii afacerii* din Anexa nr. 1 la Proiect cu un nou punct, punctul 4) cu următorul conținut: „*4) să stabilească o strategie pentru asigurarea accesului continuu la comunicațiile de urgență.*"
- completarea *Domeniului VII. Monitorizare, testare şi audit* din Anexa nr. 1 la Proiect cu un nou punct, punctul 6) cu următorul conținut: „*6) să stabilească politici de monitorizare a serviciilor asociate comunicațiilor de urgență.*"

Răspunsul ANCOM:

În ceea ce privește măsurile de securitate pe care furnizorii trebuie să le implementeze, în Anexa nr. 1 la Proiect se regăsesc obiectivele de securitate grupate pe opt domenii.

Conform *Domeniului IV. Managementul operaţiunilor* din Anexa nr. 1 la Proiect, furnizorii trebuie să stabilească și să mențină proceduri privind managementul schimbărilor efectuate în rețeaua de comunicații electronice precum și în sistemele informatice (software) pentru a minimiza probabilitatea apariției incidentelor rezultate în timpul sau în urma schimbărilor respective. Introducerea unor sisteme noi, schimbările majore aduse celor existente sau schimbări aduse unor elemente importante, trebuie să urmeze un proces de documentare, definire a cerințelor tehnice, testare, control al calității și implementare controlată. Acest proces trebuie să cuprindă o determinare a riscului, o analiză a impactului modificărilor și stabilirea măsurilor de securitate necesare. La evaluarea impactului trebuie avut în vedere, în mod evident, și impactul asupra comunicațiilor de urgență.

Prin urmare, având în vedere cele menționate anterior, ANCOM acceptă observația respondentului, iar pct. 4 din *Domeniul IV. Managementul operaţiunilor* din Anexa nr. 1 la Proiect va avea următorul conținut:

„4) să efectueze evaluări prealabile ale impactului potențial al unei schimbări de sistem;”.

Domeniul V. Managementul incidentelor din Anexa nr. 1 la Proiect are ca obiective majore stabilirea unor procese și proceduri pentru managementul incidentelor de securitate, implementarea proceselor și sistemelor de detectare a incidentelor de securitate și a evenimentelor care pot conduce la incidente, raportarea incidentelor către ANCOM și către alte autorități responsabile, precum și stabilirea planurilor de comunicare a incidentelor către alte părți externe. Procedurile trebuie să stabilească modul de abordare a diverselor tipuri de incidente, identificarea impactului unui incident (asupra serviciilor, utilizatorilor, resurselor, în funcție de localizare/arie geografică etc.), identificarea și analizarea cauzei incidentului, măsurile care pot fi luate pentru a minimiza efectele incidentului şi pentru a remedia defecțiunile care au cauzat incidentul, planificarea și implementarea acțiunilor corective pentru împiedicarea reapariției sale, comunicarea cu cei afectați de incident, colectarea probelor, dar și restabilirea funcționării serviciilor în cel mai scurt timp posibil etc. Totodată, prevederile art. 14 și 15 din Ordonanța de urgență a Guvernului nr. 34/2008 menționează obligația furnizorilor de servicii de comunicații interpersonale bazate pe numere, destinate publicului, care asigură prin intermediul reţelelor publice fixe și mobile servicii de originare a apelurilor către un număr sau numere din Planul naţional de numerotaţie ori din planurile de numerotaţie internaţionale, de a asigura, cu prioritate, primirea şi rutarea apelului de urgență. În același timp, dispozițiile art. 24^1 din Decizia președintelui ANCOM nr. 1023/2008 prevăd faptul că furnizorii de servicii de comunicații interpersonale bazate pe numere destinate publicului care asigură prin intermediul rețelelor publice servicii de originare a apelurilor către un număr sau numere din Planul național de numerotație ori din planurile de numerotație internaționale au obligația de a lua toate măsurile necesare pentru a asigura în mod neîntrerupt posibilitatea efectuării de apeluri către serviciul de urgență 112.

Având în vedere aceste obligații ale furnizorilor referitoare la comunicațiile de urgență, precum și importanța acestora pentru societate, **ANCOM acceptă propunerea respondentului și introduce un nou punct în cuprinsul *Domeniului V. Managementul incidentelor*, punctul 6), având următorul cuprins:**

„6) să stabilească procese și proceduri pentru restabilirea prioritară a serviciilor ce contribuie la realizarea comunicațiilor de urgență.”.

În conformitate cu prevederile *Domeniului VI. Managementul continuităţii afacerii* din Anexa nr. 1 la Proiect, furnizorii au obligația de a stabili o strategie pentru asigurarea continuității furnizării reţelelor şi serviciilor în situaţiile generate de perturbări grave ale funcţionării rețelei sau serviciului, inclusiv în ceea ce privește măsuri referitoare la asigurarea rezilienței lanțului de aprovizionare cu echipamente și software necesare furnizării rețelelor și serviciilor de comunicații, să deţină capabilităţi de implementare a strategiei de continuitate şi să stabilească planuri de continuitate şi de recuperare. În acest sens, pe lângă stabilirea măsurilor și politicilor adecvate pentru restabilirea cât mai repede posibil a serviciilor de rețea și de comunicații importante, se pot avea în vedere măsuri cum ar fi prioritizarea restaurării celor mai importante procese sau servicii, precum cele ce susțin comunicațiile de urgență. Caracterul important al comunicațiilor de urgență este evidențiat și de art. 62 alin. (2) din OUG nr.111/2011 care prevede explicit că *„Furnizorii de servicii de comunicații de voce au obligația de a lua toate măsurile necesare pentru a asigura acces neîntrerupt la serviciile de urgență, precum și transmiterea neîntreruptă a avertizărilor publice”*.

Prin urmare, având în vedere cele menționate anterior, **ANCOM acceptă propunerea respondentului și introduce un nou punct în cuprinsul *Domeniului VI Managementul continuităţii afacerii*, punctul 4), având următorul cuprins:**

„4) să stabilească o strategie pentru asigurarea accesului neîntrerupt la comunicațiile de urgență.”

În conformitate cu prevederile *Domeniului VII Monitorizare, testare şi audit* din Anexa nr. 1 la Proiect, furnizorii trebuie să stabilească politici de monitorizare a sistemelor, precum şi politici privind jurnalele de sistem care să asigure vizibilitate adecvată, să detecteze anomalii, să identifice și să prevină amenințări, să stabilească politici pentru testarea planurilor de continuitate şi de recuperare în cazul perturbărilor grave ale funcţionării reţelei sau serviciului, să stabilească politici pentru testarea echipamentelor, sistemelor, software-lor și corecțiilor software înainte de conectarea/punerea lor în funcţiune/implementarea lor, să stabilească o politică pentru evaluarea şi testarea securităţii tuturor resurselor (echipamente, sisteme şi software etc.). Acest proces de monitorizare trebuie să includă și infrastructura utilizată pentru comunicațiile de urgență.

Având în vedere cele menționate anterior, precum și importanța efectuării comunicațiilor de urgență de către utilizatorii finali, **Autoritatea acceptă propunerea respondentului; punctul 1) din cuprinsul *Domeniului VII. Monitorizare, testare şi audit* din Anexa nr. 1 la Proiect se va completa și va avea următorul cuprins:**

„1) să stabilească politici de monitorizare a sistemelor, precum şi politici privind jurnalele de sistem care să asigure vizibilitate adecvată, să detecteze anomalii, să identifice și să prevină amenințări, inclusiv în ceea ce privește asigurarea comunicațiilor de urgență;

12. Pentru a adăuga mai multă claritate și substanță prevederilor referitoare la dependența de un singur producător din Anexa nr. 1 la Proiect, un respondent solicită completarea prevederilor de la pct. 2) lit. b) din cuprinsul *Domeniului I Politica de securitate și managementul riscului* din Anexa nr. 1 la Proiect cu următorul conținut: *„b) să identifice riscurile, prin identificarea resurselor, amenințărilor, vulnerabilităților, măsurilor existente şi a consecințelor pe care incidentele de securitate le-ar putea avea asupra resurselor și să se asigure că personalul de conducere este informat în mod corespunzător despre aceste riscuri, dar și despre măsurile de reducere a lor; în cazul rețelelor definite la art. 2 lit. f) din Legea nr. 163/2021, se vor avea în vedere, totodată, potențiale riscuri cauzate de expunerea la terțe părți considerate a prezenta un grad de risc ridicat, ori dependența de un singur producător, pe baza unui proces de management al riscului transparent, luând în considerare viabilitatea comercială și tehnică, aspecte legate de termenele și condițiile acordurilor comerciale existente cu producătorul, poziția în piață a acestuia, alți factori;”*.

Răspunsul ANCOM:

Atât cadrul de reglementare european, cât și legislația primară națională, precum și Proiectul și numeroasele ghiduri europene (parte din ele menționate în expunerea de motive la Proiect) prevăd ca măsurile de securitate concrete pe care furnizorii le stabilesc să fie precedate de o analiză de risc. Acest aspect este reflectat și în conținutul art. 3 alin. (1) – (3) din Proiect. În conformitate cu aceste dispoziții, furnizorii au obligația de a lua toate măsurile de securitate - atât tehnice, inclusiv criptarea, după caz, cât și organizatorice - adecvate, obiective și proporționale pentru a gestiona în mod corespunzător riscurile la adresa securității rețelelor și serviciilor de comunicații electronice, astfel încât să asigure un nivel de securitate corespunzător riscului identificat ținând seama de stadiul actual al tehnologiei și să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor și asupra altor rețele și servicii. Măsurile de securitate pe care trebuie să le stabilească și să le implementeze furnizorii vor viza cel puțin domeniile și obiectivele identificate în anexa nr. 1.

Domeniul I. Politica de securitate şi managementul riscului este cel care abordează aspecte ce se referă la stabilirea unor măsuri constând în existența unei politici de securitate la nivelul organizației, stabilirea unui management al riscului (având în vedere că măsurile de securitate adecvate sunt bazate pe analiza de risc), politici cu privire la cerințele de securitate atât pentru achiziționarea de la terțe părți de produse și servicii (identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate), fiind astfel și cel mai granular dintre toate domeniile.

Cu privire la solicitarea completării prevederii de la pct. 2) lit. b) din cuprinsul *Domeniului I*, facem precizarea că obiectivul întregului domeniu este stabilirea unui proces de management al riscului ce trebuie să respecte cerințele menționate de Proiect. Așadar, considerăm scopul primei

completări propuse de respondent în textul de la lit. b) *(„...pe baza unui proces de management al riscului transparent...”*) ca fiind deja atins prin Proiect în forma sa actuală.

În ceea ce privește continuarea completării (*„...luând în considerare viabilitatea comercială și tehnică, aspecte legate de termenele și condițiile acordurilor comerciale existente cu producătorul, poziția în piață a acestuia, alți factori.”*), facem precizarea că textul deciziei conține numeroase prevederi în acest sens. În conformitate cu acestea, furnizorii vor avea obligația de a include cerințe de securitate în contractele pentru achiziţionarea de la terţe părţi de produse şi servicii (identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate), pentru asigurarea întreţinerii sau gestiunii de către terţe părţi a acestor produse şi servicii, inclusiv în ceea ce privește confidențialitatea și transferul securizat al informației, să țină evidența incidentelor de securitate cauzate de terțe părți, să ia măsuri pentru a reduce riscurile reziduale care nu au fost adresate de terțele părți sau sunt rezultate din interacțiunea cu acestea. În plus, în conformitate cu pct. 6), în cazul rețelelor 5G, obligațiile referitoare la lanțul de aprovizionare sunt sporite, având în vedere riscurile suplimentare identificate la nivel european.

Având în vedere motivele expuse mai sus, Autoritatea respinge această observație, precum și propunerea de completare formulată de către respondent.

13. Un respondent solicită eliminarea din textul Proiectului a obligațiilor stipulate la pct. 6, literele a)-d) din *Domeniul I Politica de securitate şi managementul riscului* din Anexa nr. 1 la Proiect, întrucât respectivele obligații, referitoare la achiziția de echipamente, nu pot fi respectate de către furnizori. În susținerea solicitării sale, respondentul face trimitere la procesul certificării, desfășurat de organisme special constituite, care nu poate fi substituit prin efectuarea unor verificări de către furnizori, care nu au nici resursele și nici expertiza necesare în acest scop. Respondentul atrage atenția că, prin aplicarea Legii nr. 163/2021, numărul producătorilor a fost deja restrâns, existând posibilitatea ca producătorii rămași să nu dețină astfel de certificări, mai ales că sistemele europene de certificare a securității cibernetice la care face referire litera a) de la pct. 6 din Domeniul I nu sunt finalizate. Prin urmare, Proiectul nu ar putea să impună decât obligația de a achiziționa echipamente certificate de organismele instituite în acest scop, iar obligația nu ar putea să devină aplicabilă decât în măsura în care pe piața din România ar exista cel puțin doi producători certificați.

Cu privire la pct. 6) lit. a) din *Domeniul I Politica de securitate şi managementul riscului* din Anexa nr. 1 la Proiect, un alt respondent a menționat importanța necesității utilizării unui regulament cadru de certificare unitar la nivelul Uniunii Europene și evitarea fragmentării acestuia la nivelul Statelor Membre sau al altor instituții. Nu a făcut propuneri de modificare, ci a subliniat importanța existenței fragmentului de text din Proiect *„în cazul în care astfel de sisteme de certificare sunt obligatorii”*.

Răspunsul ANCOM:

În ceea ce privește prevederile de la pct. 6), trebuie avut în vedere că obiectivul principal îl constituie asigurarea securității produselor şi serviciilor achiziționate de la părți externe, accesate sau administrate de către terți și totodată de a asigura nivelul de securitate adecvat, precum și acela de a crea garanția că dependențele de terțe părți nu afectează securitatea rețelelor și serviciilor de comunicații electronice. Aceste prevederi nu pot fi eliminate, mai ales în contextul în care la nivel european există o preocupare semnificativă în acest sens.

Relevante sunt în primul rând prevederile măsurii tehnice TM 08 (*raising the security standards in suppliers' processes through robust procurement conditions*) și cele ale TM 09 (*using EU certification for 5G network components, customer equipment and/or suppliers' processes*) din *Setul de Instrumente al UE pentru Securitatea Rețelelor 5G*[18]. TM 08 introduce cerința de a solicita de la producătorii de echipamente, în cadrul procedurilor de achiziții derulate de către furnizori, a standardelor de securitate. Riscurile urmărite sunt cele provenite din calitatea scăzută a produselor sau din exploatarea ilicită a rețelelor 5G de către diverse entități. TM 09 prevede utilizarea sistemelor europene de certificare pentru elementele de rețea 5G, echipamentele utilizatorilor și/sau proceselor furnizorilor. *Setul de instrumente* și recomandările sale cheie au fost aprobate de Comisia Europeană

[18] Disponibil la adresa: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

și acceptate de Statele Membre. În octombrie 2020, Consiliul European a cerut Uniunii Europene și Statelor Membre *să folosească pe deplin setul de instrumente pentru securitatea cibernetică 5G, adoptat la 29 ianuarie 2020,* Comisia Europeană monitorizând în acest sens implementarea *Setului de instrumente*[19].

Referitor la observația respondentului cu privire la certificare, înțelegem că aceasta vizează prevederile de la pct. 6) lit. a). Textul implică existența la nivelul organizației a unei politici cu privire la cerințele care trebuie îndeplinite pentru achiziționarea de la terțe părți de produse şi servicii (identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la apariția unor incidente de securitate) şi pentru asigurarea întreţinerii sau gestiunii de către terţe părţi a acestor produse şi servicii, care trebuie să conțină anumite elemente. Așa cum este formulat textul de la lit. a), reiese faptul că se referă la sistemele europene de certificare stabilite prin Regulamentul (UE) 2019/881 și numai dacă sunt obligatorii în virtutea legii. Procesul certificării de produs, desfășurat de organisme special constituite, nu va trebui să fie substituit de efectuarea unor verificări de către furnizori.

Textul lit. a) din Proiect nu instituie o obligație de certificare în sarcina furnizorilor sau a producătorilor de echipamente.

Prin urmare, având în vedere observațiile respondenților, pentru clarificarea prevederilor lit. a) de la pct. 6) din *Domeniul I. Politica de securitate şi managementul riscului* din Anexa nr. 1 la Proiect și a situațiilor în care aceste certificate sunt obligatorii, ANCOM va reformula textul acestei litere după cum urmează:

„ a) referitor la echipamentele identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate, obligația achiziționării unor echipamente puse la dispoziție de terțele părți, precum și a proceselor și serviciilor acestora (procese TIC, servicii TIC, produse TIC, echipamente din componența rețelelor definite la art. 2 lit. f) din Legea nr. 163/2021, servicii cloud etc.) certificate în conformitate cu sistemele europene de certificare aplicabile, în cazul în care astfel de sisteme de certificare prevăzute de Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) sunt obligatorii în temeiul dreptului național sau european."

În ceea ce privește propunerea de eliminare a lit. b) – d), Autoritatea constată că respondentul nu a prezentat argumente în favoarea acesteia.

Reiterăm faptul că, așa cum este formulat pct. 6), acesta implică existența la nivelul organizației a unei politici cu cerințe pentru achiziţionarea de la terţe părţi de produse şi servicii, furnizorul având posibilitatea transferului diligențelor în sarcina terților (de exemplu, prin clauze contractuale, solicitare de declarații pe proprie răspundere, certificate de conformitate, auditarea terților, prezentarea unor secțiuni relevante extrase din propriile lor proceduri interne, prin compensații financiare în cazul în care sistemele livrate nu sunt sigure, stabilirea unor indicatori de performanță care se monitorizează și se raportează periodic - SLA etc). Pentru a veni în sprijinul părților interesate, precizăm că ISO/IEC 27002:2022 conține informații relevante în ceea ce privește securitatea lanțului de aprovizionare, rolul furnizorului în relația cu terții lui, la următoarele secțiuni: *5.14 Transferul informațiilor, 5.19 Securitatea informației în relațiile cu furnizorii, 5.20 Abordarea securității informației în cadrul acordurilor cu furnizorii, 5.21 Managementul securității informației în lanțul de aprovizionare TIC, 5.22 Monitorizarea, revizuirea și managementul schimbării serviciilor furnizorilor, 5.23 Securitatea informației pentru utilizarea serviciilor cloud, 6.6 Acorduri de confidențialitate și nedezvăluire, 8.8 Managementul vulnerabilităților tehnice, 8.30 Dezvoltare externalizată*. Menționăm că și în prezent practica din piață referitoare la achizițiile desfășurate de organizații mari prin propriile departamente de achiziții prevede precalificarea furnizorilor/producătorilor prin prezentarea unui set de documente

[19] Al doilea raport privind progresele înregistrate publicat la adresa: https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

și completarea unor chestionare. Prin intermediul obiectivelor de securitate de la pct. 6) se creează un cadru legal care încurajează comunicarea și colaborarea pentru a minimiza/elimina efectele incidentelor de securitate.

Având în vedere motivele expuse mai sus, Autoritatea respinge aceste observații referitoare la eliminarea lit. a)-d) de la pct. 6) din *Domeniul I. Politica de securitate şi managementul riscului* din Anexa nr. 1 la Proiect.

14. Un respondent solicită eliminarea din cadrul prevederilor punctului 2 al *Domeniului III Securitatea reţelelor şi serviciilor, a facilităţilor asociate şi a informaţiilor* din Anexa nr. 1 la Proiect a tuturor mențiunilor care ar impune măsuri stricte de control și monitorizare a accesului fizic la rețelele definite la art. 2 lit. f) din Legea nr. 163/2021 – în sensul de măsuri care ar presupune procese automatizate, această activitate urmând să facă în continuare obiectul unor procese de implementare punctuale, în concordanță cu necesitățile și riscurile identificate la nivel intern de către furnizorii de rețele. Respondentul consideră măsura ca fiind excesivă și lipsită de proporționalitate, instituirea obligației de monitorizare a accesului fizic la nivelul miilor de stații de bază existente la nivelul unei rețele reprezentând, în opinia respondentului, o sarcină extrem de împovărătoare pentru furnizori.

Răspunsul ANCOM:

Așa cum a fost formulat textul de la pct. 2 din *Domeniul III Securitatea reţelelor şi serviciilor, a facilităţilor asociate şi a informaţiilor* din Anexa nr. 1 la Proiect, reiese că măsurile de securitate efective se vor stabili în conformitate cu importanța obiectivului protejat și vor ține cont de riscurile specifice. În acest sens, Autoritatea subliniază faptul că nu urmărește instituirea unei obligații de monitorizare în timp real a accesului fizic la nivelul tuturor stațiilor de bază existente la nivelul unei rețele, mai ales în cazul celor unde nu se justifică o asemenea măsură. Cu toate acestea, în cazul în care stațiile de bază conțin, de exemplu, componente *multi-access edge computing* sau în cazul hub-urilor de transmisiuni, securitatea acestora ar trebui sporită cu măsuri suplimentare. Măsurile de securitate sunt stabilite de către furnizori, în urma evaluării propriilor riscuri, cu respectarea principiului proporționalității. În vederea clarificării acestei măsuri, **Autoritatea a evaluat propunerile respondentului și a decis reformularea punctului 2 din *Domeniul III Securitatea reţelelor şi serviciilor, a facilităţilor asociate şi a informaţiilor* din Anexa 1 la Proiect, după cum urmează:**

„2) în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, să stabilească măsuri de securitate suplimentare pentru accesul fizic la rețea și la facilitățile asociate, în conformitate cu importanța obiectivului protejat; măsurile de securitate vor ține cont de riscurile specifice acestor rețele, inclusiv cele generate de accesul părților terțe."

15. Un respondent solicită completarea punctului 5 al *Domeniului III Securitatea reţelelor şi serviciilor, a facilităţilor asociate şi a informaţiilor* din Anexa nr. 1 la Proiect, în scopul de a întări alinierea la recomandările UE, astfel:

„5) în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, se vor implementa măsuri de securitate suplimentare, în concordanță cu reglementările și recomandările la nivelul Uniunii Europene, care vor ține cont de riscurile specifice ale acestor rețele. Controlul strict al accesului și/sau restricționarea accesului vor fi avute în vedere în cazul terților sau furnizorilor de servicii gestionate care sunt considerați de risc ridicat sau care accesează din țări din afara Uniunii Europene rețelele și sistemele informatice."

Răspunsul ANCOM:

Autoritatea consideră că scopul propunerii este unul legitim, mai ales în contextul în care Statele Membre au în vedere din ce în ce mai mult ghidurile, recomandările, studiile, bunele practici emise la nivelul instituțiilor europene. În acest sens, au fost indicate, fără a constitui o listă exhaustivă, atât în expunerea de motive, cât și în răspunsurile formulate în prezenta sinteză, câteva documente relevante pentru Proiect.

Însă, având în vedere că la art. 46 alin. (4) din Ordonanța de urgență a Guvernului nr. 111/2011 se prevede că *„(4) Măsurile luate potrivit alin. (1) vor avea în vedere, în mod corespunzător, recomandările și ghidurile de bune practici elaborate de ANCOM și pe cele elaborate de Agenția Uniunii Europene pentru Securitate Cibernetică, denumită în continuare ENISA"*, Autoritatea consideră obiectivul propunerii primite ca fiind atins, fără a fi necesare ajustări suplimentare pe text.

Având în vedere motivele expuse mai sus, Autoritatea respinge această observație, precum și propunerea de modificare formulată de către respondent.

În același timp, ținând cont de modificările realizate la pct. 2 din cuprinsul *Domeniului III Securitatea reţelelor şi serviciilor, a facilităţilor asociate şi a informaţiilor* din Anexa nr. 1 la Proiect menționate anterior, pentru clarificarea domeniului de aplicare a pct. 5, **Autoritatea completează textul acestui punct, astfel încât acesta să reflecte în mod evident faptul că se aplică în cazul accesului logic la rețelele definite la art. 2 lit. f) din Legea nr. 163/2021:**

„5) în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, se vor implementa măsuri de securitate suplimentare pentru accesul logic care vor ține cont de riscurile specifice ale acestor rețele. Controlul strict al accesului și/sau restricționarea accesului vor fi avute în vedere în cazul terților sau furnizorilor de servicii gestionate (entitățile care furnizează servicii legate de instalarea, gestionarea, funcționarea sau întreținerea produselor, rețelelor, infrastructurii, aplicațiilor TIC sau a oricăror alte rețele și sisteme informatice, prin intermediul asistenței sau al administrării active efectuate fie la sediul clienților, fie la distanță) care sunt considerați de risc ridicat sau care accesează din țări din afara Uniunii Europene rețelele și sistemele informatice;"

16. Doi respondenți formulează observații la punctul 4 al *Domeniului V Managementul incidentelor* din Anexa nr. 1 la Proiect, referitor la centrele de operațiuni. Un respondent solicită să fie prevăzut că centrele de operațiuni pot funcționa fie în perimetrele proprii ale furnizorilor (în cazul în care aceștia desfășoară activitatea de operare a rețelei), fie în perimetrul terților autorizați (în situația în care activitatea de operare a fost externalizată). Având în vedere că mulți furnizori de rețele, atât la nivelul Uniunii Europene, cât și la nivel național, au atribuit activitatea de operare a rețelelor unor terți parteneri, centrele de operațiuni de rețea și/sau centrele de operațiuni de securitate funcționează de regulă în perimetrele respectivilor parteneri. Celălalt respondent solicită eliminarea referinței la teritoriul național și menținerea doar a cerinței ca centrele de operațiuni și de securitate să funcționeze în perimetrele proprii de pe teritoriul Uniunii.

Răspunsul ANCOM:

Pentru a clarifica textul și a evita ambiguitățile, având în vedere și observația respondentului, textul de la pct. 4) al Domeniului V Managementul incidentelor din Anexa nr. 1 la Proiect a fost revizuit și va avea următorul conținut: *„4) în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, centrele de operațiuni de rețea și/sau centrele de operațiuni de securitate vor funcționa pe teritoriul național și/sau pe teritoriul Uniunii Europene; acestea ar trebui să asigure vizibilitatea și monitorizarea componentelor rețelei respective pentru a detecta evenimente de securitate și pentru a identifica și preveni amenințări.*"