Proiectul de lege 5G[1] - de ce este necesară adoptarea unor criterii tehnice pentru asigurarea securității cibernetice?

Nevoia statelor de a reglementa noi măsuri prin care să fie asigurată securitatea rețelelor de comunicații nu este nouă, însă, în perioada recentă au fost dezbătute public mai multe inițiative legislative, precum și expuneri ale unor documente politice în acest domeniu.

Proiectul de lege pentru transpunerea codului european ala comunicațiilor[2] aduce amendamente inclusiv în Capitolul IV referitor la securitatea rețelelor și serviciilor de comunicații electronice, politica Uniunii Europene în acest domeniu cunoscând, astfel, o nouă orientare în ceea ce privește securitatea cibernetică a rețelelor 5G. Printre acestea, **caracterul adecvat și proporțional al măsurilor de securitate este circumstanțiat de stadiului actual al tehnologiei**, ceea ce va impune adaptarea practicilor de securitate în funcție de evoluțiile tehnologice. În același sens, se propune ca furnizorii de rețele publice de comunicații electronice să aibă în vedere ghidurile de bune practici elaborate de ANCOM și de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA).

În privința noii tehnologii de comunicații – 5G, autoritățile naționale și europene au înțeles să propună măsuri specifice pentru asigurarea securității rețelelor. Setul Comun de Instrumente 5G al UE (5G EU Toolbox) conține o serie de **măsuri tehnice și strategice** propuse spre implementare statelor membre ale Uniunii Europene.

Prin Setul Comun de Instrumente 5G al UE, se arată, explicit, că **riscul generat de către furnizorii de echipamente ar putea fi evaluat inclusiv prin raportare la calitatea produselor și a practicilor de securitate cibernetică ale producătorilor.**

De altfel, în România, observăm că politica de securitate cibernetică rămâne atașată ideii de **certificare a soluțiilor tehnologice**, o hotărâre recentă a Camerei Deputaților în acest domeniu, respectiv, Hotărârea Camerei Deputaților nr. 40/31.03.2021 subliniind ca produsele pentru digitalizare să fie supuse **unor standarde și norme de securitate cibernetică încă din faza de proiectare.**

De asemenea, Camera Deputaților, care va fi și prima Cameră sesizată cu dezbaterea proiectului de lege, „ *(…) consideră necesară elaborarea unor standarde și norme de securitate cibernetică ce trebuie implementate integrat în contextul transformării digitale ca parte a Mecanismului de redresare și reziliență*;”. Concluzia care poate fi dedusă din aceste reglementări nu poate fi decât aceea că nu putem asigura securitate cibernetică „în abstract” ci numai în concret, prin raportare, în primul rând, la criterii tehnice care să ne ofere certitudinea că un produs sau serviciu este sigur încă din faza de proiectare.

---

[1] Proiectul de Lege privind adoptarea unor măsuri referitoare la infrastructuri informatice și de comunicații de interes național și condițiile implementării rețelelor 5G, aflat în prezent pe agenda de lucru a Guvernului. Ultima versiune a Proiectului de Lege este cea din publicată în data de 13.04.2021 la https://sgg.gov.ro/1/proiectele-de-acte-normative-care-ar-putea-fi-incluse-in-sedinta-guvernului-romaniei-din-15-04-2021/

[2] Versiunea îmbunătățită publicată de Ministerul Transporturilor si Infrastructurii în data de 19.03.2021.

Importanța implementării unitare, la nivelul Uniunii Europene, a măsurilor prevăzute de Manualul Uniunii Europene este subliniată atât de către Consiliul European[3], cât și de către Comisia Europeană[4], care încurajează statele membre să aplice criterii obiective comune în evaluarea furnizorilor de produse și software ce ar urma a fi folosite în implementarea tehnologiei 5G. În plus, această măsură este orientată numai către acele „*active de bază definite ca fiind esențiale și sensibile în evaluările coordonate ale riscurilor la nivelul UE*".

Cu toate că în expunerea de motive a *Proiectului de Lege privind adoptarea unor măsuri referitoare la infrastructuri informatice și de comunicații de interes național și condițiile implementării rețelelor 5G* se menționează că ar lua in considerare evaluările de risc de la nivel european și recomandările din Setul Comun de Instrumente 5G al UE de adresare a riscurilor și vulnerabilităților non-tehnice aferente lanțului de aprovizionare, criteriile propuse a fi avute în vedere pentru evaluarea producătorilor sunt diferite de cele menționate în Setul Comun de Instrumente 5G al UE.

Astfel cum a fost reținut și de către instituțiile avizatoare ale proiectului, pe parcursul procedurii legislative, respectiv, de către Ministerul Justiției prin avizul nr. 2/88892/2020/15.10.2020 și de către Consiliul Legislativ prin avizul nr. 202 din 08.04.2021, aceste criterii sunt neclare, imprecise și imprevizibile.

Or, lipsa unor criterii de evaluare precise si cuantificabile înlătură orice certitudine că un produs sau serviciu este sigur și poate fi utilizat pe piață.

Dincolo de asigurarea a însuși dezideratului securității cibernetice, absența unor criterii obiective și proporționale cu scopurile urmărite de către inițiatori, ar putea reprezenta vicii de neconstituționalitate ale legii. Astfel, în lipsa unor criterii obiective și proporționale, este pusă la îndoială respectarea principiului legalității și a principiului securității raporturilor juridice în contextul în care redactarea actuală a proiectului de lege tinde să acorde autorităților publice o marjă discreționară de apreciere și să lipsească producătorii de echipamente de o protecție adecvată împotriva arbitrariului. Totodată, se pune problema încălcării condițiilor pentru restrângerea exercițiului unor drepturi și libertăți fundamentale prevăzute de art. 53 din Constituția României, în măsura în care aceste criterii ar fi menținute de către Parlament.

Existența unor potențiale vicii de neconstituționalitate din perspectiva nerespectării principiului legalității este semnalată și în avizul Consiliului Legislativ nr. 202 din data de 08.04.2021, însă aceste observații nu au fost avute în vedere de inițiatori, după cum reiese din versiunea actualizată a Proiectului de lege, publicată în data de 13.04.2021.

De asemenea, proiectul de lege propus se îndepărtează atât de viziunea actuală care, presupune în primul rând o evaluare a securității produselor, cât și de Setul Comun de Instrumente 5G al UE, care propune evaluarea producătorilor inclusiv prin raportare la calitatea produselor și a practicilor de securitate cibernetică.

Este de remarcat că în prezent există un cadru de reglementare general în materia securității la nivelul Uniunii Europene, respectiv, Directiva NIS (Directiva (UE) 2016/1148 A Parlamentului European și a Consiliului), aflată în proces de revizuire, precum și alte acte normative aplicabile în domenii speciale, cum ar fi norme specifice pentru asigurarea securității datelor cu

---

[3]Concluziile Consiliului European din 1-2 octombrie 2020 disponibile la https://www.consilium.europa.eu/ro/meetings/european-council/2020/10/01-02/

[4] Comunicare Comună către Parlamentul European și Consiliu Strategia de securitate cibernetică a UE pentru deceniul digital disponibilă la https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52020JC0018

caracter personal în GDPR ori norme speciale în cuprinsul Codului European al Comunicațiilor Electronice[5], în privința rețelelor de comunicații electronice.

Cât privește comunicațiile electronice, O.U.G nr. 111/2011, în forma actuală, plasează în sarcina furnizorilor de rețele publice de comunicații electronice obligația de a lua toate măsurile tehnice și organizatorice adecvate pentru a administra riscurile care pot afecta securitatea rețelelor și serviciilor. Încălcarea acestei obligații de către furnizorii de rețele publice de comunicații electronice poate atrage răspunderea contravențională a acestora.

Reglementarea primară mai sus enunțată este completată cu Decizia președintelui ANCOM nr. 512/2013 care detailează coordonatele în care furnizorii de servicii de rețele publice de comunicații electronice au obligația de a asigura măsurile tehnice și organizatorice adecvate. Aceste măsuri presupun inclusiv stabilirea unor politici pentru testarea echipamentelor, a sistemelor si software-ului, în special înainte de conectarea/punerea lor in funcțiune și stabilirea unei politici adecvate pentru evaluarea și testarea securității tuturor resurselor, respectiv a echipamentelor, sistemelor și software-ului.

În acest context, s-ar putea concluziona că excluderea oricărei evaluări tehnice a producătorilor, astfel cum este propus prin Proiectul de Lege, contribuie la crearea unui cadru normativ neclar și la încălcarea actelor normative adoptate la nivelul Uniunii Europene în materia comunicațiilor electronice care obligă la obiectivitate, certitudine, consecvență și previzibilitate, precum și la nediscriminare, proporționalitate și transparență.

Av. Ion Dragne

[5] Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018