ANCOM | Autoritatea Națională pentru Administrare și Reglementare în Comunicații

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

Către,

PARLAMENTUL ROMÂNIEI - SENAT

În atenția domnului **Mario Ovidiu OPREA**, Secretar General

Subiect: avizarea propunerii legislative privind evidența și administrarea infrastructurii digitale publice, precum și pentru crearea Platformei naționale a infrastructurii digitale publice (b607/2025).

Stimate domn Secretar General,

L651/2025

Urmare a adresei dumneavoastră nr. 6572/24.11.2025, înregistrată în cadrul Autorității Naționale pentru Administrare și Reglementare în Comunicații (în continuare, *ANCOM* sau *Autoritate*) cu nr. SC-26096/28.11.2025, prin care ne transmiteți propunerea legislativă privind evidența și administrarea infrastructurii digitale publice, precum și pentru crearea Platformei naționale a infrastructurii digitale publice,

În temeiul art. 2 alin. (1), art. 4 alin. (3), art. 5 lit. b), 10 alin. (1) pct. 7 din Ordonanța de urgență a Guvernului nr. 22/2009 privind înființarea Autorității Naționale pentru Administrare și Reglementare în Comunicații, aprobată prin Legea nr. 113/2010, cu modificările și completările ulterioare, vă transmitem următoarele observații:

Obiectul normei, astfel cum este formulat în art. 1 alin. (2) din propunerea legislativă, respectiv crearea, operaționalizarea și administrarea Platformei naționale a infrastructurii digitale publice (*PNIDP*) ca instrument unic de evidență, coordonare și supraveghere a infrastructurii digitale publice, este, în opinia noastră, susceptibil de a genera ambiguitate în interpretarea și aplicarea sa. Astfel, estimăm că utilizarea sintagmei *„supravegherea infrastructurii digitale publice"*, în lipsei unei definiții conceptuale explicite, este de natură să tangențieze fie cu regimul comunicațiilor electronice (instituit prin Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată, cu modificări și completări, prin Legea nr. 140/2012, cu modificările și completările ulterioare, în ceea ce privește furnizarea rețelele publice de comunicații electronice sau serviciile de comunicații electronice destinate publicului, respectiv relația furnizor – utilizator final), fie cu normele privind securitatea cibernetică (regimul NIS2[1], care instituie, în principiu, măsuri *„adecvate și proporționale cu riscul"*, premisă care nu se regăsește în obligațiile impuse la punctul 1 al Anexei 1 din propunerea legislativă (*„Autentificare cu doi factori (MFA) pentru toți utilizatorii"*, *„Configurarea obligatorie a SPF, DKIM și DMARC (politica „reject")"*, cerințe fixe de backup/restore, etc.). Nu în ultimul rând, parte din cerințele individualizate în cuprinsul Anexei 1 și 2 (utilizarea formatelor deschise: CSV, XML, JSON, ODF fără criptare, implementarea

[1] Ordonanță de Urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, aprobată, cu modificări și completări, prin Legea nr. 140/2012, act care transpune Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2).

infrastructurilor digitale publice în Cloudul Guvernamental sau în centre de date certificate, procesarea datelor de contact ale responsabilului digital al entității publice, administratorul tehnic, altul decât responsabilul digital, dacă este cazul) pot intra în conflict și cu regimul ePrivacy[2], dacă vor conduce la „vederea" meta-datelor comunicațiilor sau identificarea utilizatorilor finali. Avem în vedere faptul că o conformare cu obligațiile nou instituite în cele două anexe poate genera un conflict de aplicare cu dispozițiile art. 4 alin. (2) sau ale art. 5 alin. (1) din Legea 506/2004[3], întrucât se pot accesa meta-date de comunicare (volum, timpi, surse/destinații la nivel de infrastructură) sau informații private („cine comunică", „cât comunică"), în contradicție cu condițiile specifice de garantare a dreptului la protecția vieții private în sectorul comunicațiilor electronice, prin care se interzice supravegherea/prelucrarea comunicațiilor și datelor de trafic fără consimțământ/temei sau, dacă vorbim de date de trafic, prelucrarea datelor de trafic limitată, în principal de furnizori, și în scopuri strict determinate.

În plus față de cele expuse, este posibil ca PNIDP să impună o arhitectură de securitate mai strictă decât ar rezulta din analiza de risc NIS 2 pentru unele sisteme (și, uneori, chiar nepotrivită tehnologic).

Față de cele expuse mai sus, apreciem că se impune reformularea textului propunerii legislative, astfel încât să se instituie în mod explicit faptul că: *„Supravegherea infrastructurii digitale publice se realizează exclusiv pe baza informațiilor administrative declarate de entitățile publice, fără acces la sistemele informatice, la traficul de date, la conținutul comunicațiilor sau la datele cu caracter personal."* Cumulativ, se impune modificarea punctului 1 al Anexei nr. 1 din propunerea legislativă, în ceea ce privește obligațiile referitoare la *„Autentificare cu doi factori (MFA) pentru toți utilizatorii"* și *„Configurarea obligatorie a SPF, DKIM și DMARC (politica «reject»)"*, în sensul impunerii acestora doar pentru protejarea resurselor digitale publice considerate ca fiind de importanță majoră.

În ceea ce privește corelarea propunerii legislative cu Legea nr. 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate, cu care se află în conexiune, apreciem că există un risc semnificativ ca prin dispozițiile propuse să fie depășit principiul instituit prin Regulamentul (UE) 2018/1724 al Parlamentului European și al Consiliului din 2 octombrie 2018 privind înființarea unui unic portal digital (gateway) pentru a oferi acces la informații, la proceduri și la servicii de asistență și de soluționare a problemelor și de modificare a Regulamentului (UE) nr. 1024/2012, referitor la unicitatea sursei de acces la informații.

Avem în vedere faptul că, potrivit art. 2 lit. e) din propunerea legislativă, PNIDP se integrează în cloud-ul guvernamental și în Platforma națională de interoperabilitate (PNI) *„pentru a facilita schimbul de date între sisteme informatice"*. Având în vedere definiția resurselor digitale, de la art. 3 lit. h) din propunerea legislativă, și cea a sistemului informatic, de la art. 1 lit. a din Convenția de la Budapesta privind criminalitatea informatică[4], PNIDP apare că operează la nivel de guvernanță internă a infrastructurii digitale, în timp ce PNI, instituit prin Legea nr. 242/2022, privește accesul extern al utilizatorilor la informații și proceduri. Însă, dispozițiile art. 22 alin. (1) din propunerea legislativă, în măsura în care permit punerea la dispoziția cetățenilor sau diseminarea datelor gestionate prin PNIDP, impun o corelare expresă cu regimul juridic al interoperabilității stabilit de Legea nr. 242/2022. În lipsa unei delimitări exprese a destinatarilor și a scopului punerii la dispoziție a datelor, art. 22 alin. (1) din propunerea legislativă este

---

[2] Regim instituit prin Legea 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare.

[3] idem

[4] *„sistem informatic înseamnă orice dispozitiv sau un grup de dispozitive interconectate sau corelate, dintre care unul sau mai multe, în urma unui program, efectuează prelucrarea automată a datelor."*

susceptibil să fie interpretat în sensul conferirii PNIDP a unei funcții de acces sau diseminare către terți, cu potențială suprapunere față de rolul PNI ca mecanism unic pentru schimbul de date între sisteme informatice.

Pe de altă parte, aceeași dispoziție este susceptibilă să genereze obligații de raportare redundantă în sarcina autorităților publice, prin solicitarea unor date care sunt deja disponibile sau pot fi obținute prin Platforma Națională de Interoperabilitate, cu afectarea principiului colectării unice a datelor (once-only), consacrat de Regulamentul (UE) 2018/1724 și pus în aplicare la nivel național prin art. 9 din Legea nr. 242/2022.

În acest context, se impune o corelare normativă expresă, care să precizeze că (i) PNIDP nu constituie un punct de acces sau un mecanism de tip gateway pentru cetățeni sau alte categorii de utilizatori, rolul său fiind limitat la evidența și guvernanța internă a resurselor digitale publice și că (ii) datele gestionate prin PNIDP nu fac obiectul unor obligații suplimentare de raportare în măsura în care sunt deja disponibile prin Platforma Națională de Interoperabilitate.

În ceea ce privește obiectivul reutilizării software-ului finanțat din fonduri publice, stabilit prin art. 1 alin. (4) din propunerea legislativă, acesta apare că surclasează principiul reutilizării soluțiilor informatice consacrat de art. 5 alin. (1) lit. a) din Legea nr. 242/2022, precum și mecanismele de interoperabilitate instituite prin art. 3 lit. f), art. 9 și art. 11 din aceeași lege. În lipsa unei corelări exprese, există riscul instituirii unor regimuri paralele privind reutilizarea software-ului public, aspect ce contravine art. 14 alin. (2) sau art. 16 alin. (1) din Legea nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, republicată, cu modificările și completările ulterioare.

Totodată, în opinia noastră, ar prezenta utilitate o analiză de specialitate privind eventualele conexiuni legislative cu Hotărârea Guvernului nr. 841/1995 privind procedurile de transmitere fără plată și de valorificare a bunurilor aparținând instituțiilor publice, cu modificările ulterioare, sau cu Legea nr. 15/1994 privind amortizarea capitalului imobilizat in active corporale si necorporale, republicată, cu modificările și completările ulterioare, în ceea ce privește procedurile de scoatere din gestiune a bunurilor care nu mai pot fi utilizate sau amortizarea bunurilor din patrimoniul unei instituții.

Din perspectiva tehnicii legislative, apreciem necesară o simplificare a definiției prevăzute la art. 3 lit. a) din propunerea legislativă, întrucât reia și amestecă elemente care fac obiectul noțiunii de „resurse digitale publice", definită distinct la art. 3 lit. h) din proiect, generând confuzie cu privire la sfera și semnificația noțiunii reglementate. În acest sens, propunem, spre eficiență, următorul text pentru definirea infrastructurii digitale *„totalitatea resurselor digitale publice și a site-urilor, portalurilor, bazelor de date, echipamentelor hardware și proiectelor informatice utilizate de entitățile publice pentru furnizarea de servicii publice digitale;".*

În ceea ce privește norma instituită prin art. 4 alin. (3) din propunerea legislativă, care stabilește o cooperare a DNSC cu ADR și STS în gestionarea riscurilor cibernetice, **în condițiile legii**, apreciem faptul că această reglementare trebuie corelată cu art. 37 alin. (1) lit. a) din Ordonanța de urgență a Guvernului nr. 155/2024 care stabilește, pe de o parte, faptul că DNSC se consultă și cooperează cu ANCOM, în vederea asigurării unui nivel comun ridicat de securitate cibernetică la nivel național, iar pe de altă parte faptul că ANCOM reprezintă autoritatea competentă sectorial în domeniul securității cibernetice, potrivit prevederilor ordonanței de urgență în cauză, pentru sectorul *„8. Infrastructură digitală".* Prin urmare, apreciem utilă integrarea noilor dispoziții în ansamblul legislației existente relevante, prin utilizarea unei norme de trimitere.

În ceea ce privește atribuția ADR prevăzută la art. 5 lit. c) din propunerea legislativă, apreciem utilă dezvoltarea conceptuală a activității de audit a datelor pe care ADR o va realiza, nefiind precizat în text nici scopul acestui audit și nici obiectivul său (ce tip de date vor fi supuse auditului ADR), astfel încât eventualele implicații să poată fi prevăzute și analizate în mod corespunzător.

De asemenea, semnalăm faptul că dispozițiile art. 7 din propunerea legislativă instituie, prin alin. (1) și (3), obligația de înregistrare în PNIDP a tuturor resurselor digitale publice deținute, utilizate şi administrate în termen de 6 luni de la data intrării în vigoare sub sancțiunea interzicerii utilizării la expirarea termenului. Analiza acestor prevederi, în mod coroborat cu dispozițiile art. 21 alin. (1)[5] din proiect, precum și dispozițiile pct. 4. *"Cloud și infrastructură"* din cadrul Anexei 1[6], reliefează existența unui risc major din perspectiva implementării acestor măsuri generat de complexitatea infrastructurilor digitale publice existente în cadrul autorităților publice care vor trebui relocate în Cloud-ul Guvernamental, precum și de consumul semnificativ de resurse, inclusiv financiar, determinat de realizarea tuturor operațiunilor necesare pentru reluarea activității acestor infrastructuri și, eventual, pentru plata serviciilor către centrele de date certificate (acolo unde este cazul).

Propunerea ANCOM este de a elimina caracterul absolut al obligației de înregistrare prevăzută la art. 7 alin. (1), prin înlăturarea termenului „toate", astfel încât obligația să vizeze exclusiv acele resurse digitale publice a căror interoperabilitate sau difuzare, în condițiile legii, nu este de natură să afecteze exercitarea atribuțiilor entităților publice implicate, prin periclitarea secretului comercial, a datelor confidențiale sau a datelor cu caracter personal.

Se observă, de asemenea, că dispozițiile art. 7 alin. (4) din proiect instituie o interdicție privind achiziția proiectelor digitale publice[7] neînregistrate în PNIDP, în timp ce art. 7 alin. (1) din același act stabilește obligația de înregistrare exclusiv a resurselor digitale publice, noțiunile fiind definite distinct la art. 3 lit. e) (avem în vedere referința la noțiunea de infrastructură digitală publică) și lit. h) din propunerea legislativă. Această diferență de obiect al reglementării pare să conducă la o lipsă de corelare între ipoteza normei și consecința juridică instituită, în măsura în care se condiționează achiziția unui proiect de îndeplinirea unei obligații de înregistrare care, potrivit definițiilor legale, vizează o categorie diferită de obiecte. O asemenea formulare este de natură să creeze incertitudine cu privire la sfera de aplicare a normei, fiind necesară clarificarea textului, în acord cu cerințele art. 36 alin. (1) din Legea nr. 24/2000.

Se apreciază, de asemenea, necesară integrarea dispozițiilor art. 8 alin. (1) lit. a) din propunerea legislativă în ansamblul legislației în vigoare, în conformitate cu art. 13 din Legea nr. 24/2000, prin reconsiderarea noțiunii de *„date publice"*, în corelare cu definiția informațiilor de interes public prevăzută la art. 2 lit. b) din Legea nr. 544/2001 privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare.

În acest sens, putem exemplifica situația ANCOM care administrează, în exercitarea atribuțiilor lor legale, resurse digitale utilizate în activitatea de reglementare, reprezentare

---

[5] *„Toate resursele digitale publice înscrise în PNIDP trebuie să respecte standardele tehnice minime prevăzute în anexa nr. 1".*

[6] *"Infrastructurile digitale publice se implementează în Cloudul Guvernamental sau în centre de date certificate"*

[7] Care sunt definite, potrivit art. 3 lit. e) din propunere, ca fiind orice *"inițiativă de creare, dezvoltare, extindere sau modernizare a infrastructurii digitale publice utilizate pentru furnizarea de servicii publice digitale, finanțată din fonduri ale bugetului de stat sau fonduri europene, indiferent de cuantumul acestora și de mecanismul de cofinanțare".*

instituțională internațională sau soluționare a litigiilor între furnizorii de rețele și/sau servicii de comunicații electronice[8], iar dezvăluirea publică a existenței sau a scopului acestor resurse poate aduce atingere exercitării atribuțiilor legale, prin afectarea regimurilor juridice aplicabile confidențialității, secretului comercial ori protecției datelor cu caracter personal.

În consecință, se impune circumstanțierea datelor supuse regimului prevăzut la art. 8 alin. (1) lit. a) la acele date aferente resurselor digitale publice care privesc activitățile autorităților publice sau rezultă din acestea și a căror diseminare nu este de natură să compromită principiile confidențialității, secretului comercial ori protecției datelor cu caracter personal.

Cu privire la conținutul datelor aferente resursei digitale publice ce urmează a fi înscrise în registrul specializat prevăzut la art. 10 din proiectul normativ, se observă că solicitarea de la alin. (1) lit. e), respectiv consemnarea dovezii juridice a *„deținerii sau a dreptului de utilizare, după caz"*, precum și dispozițiile alin. (2), necesită o clarificare suplimentară. În acest sens, se are în vedere faptul că, în cazul anumitor licențe software sau aplicații, deținerea sau dreptul de utilizare nu presupun un titlu juridic distinct, utilizarea acestora fiind permisă prin simplul acces la condițiile de licențiere sau la aplicația respectivă. În lipsa unei precizări corespunzătoare (a ceea ce poate fi calificat drept dovada juridică), norma poate genera dificultăți de aplicare, contrar cerințelor de claritate și previzibilitate prevăzute la art. 36 alin. (1) din Legea nr. 24/2000.

În ceea ce privește dispozițiile art. 16 alin. (3) din propunerea legislativă, se apreciază necesară evitarea unui paralelism normativ și asigurarea corelării cu regimul juridic al raportării incidentelor de securitate cibernetică, astfel cum este reglementat la art. 15–16 din Ordonanța de urgență a Guvernului nr. 155/2024. În acest sens, se propune utilizarea unei norme de trimitere, în conformitate cu art. 16 din Legea nr. 24/2000, în vederea stabilirii cadrului aplicabil raportării incidentelor de securitate cibernetică.

Nu în ultimul rând, se observă că anumite dispoziții ale propunerii legislative, respectiv cele cuprinse la art. 17 alin. (4), art. 20 alin. (1), art. 21 alin. (1), precum și art. 25 alin. (1) și (3), sunt de natură să afecteze exercitarea atribuțiilor de reglementare ale ANCOM, autoritate publică autonomă cu personalitate juridică, aflată sub control parlamentar[9]. În măsura în care aceste dispoziții instituie obligații sau mecanisme susceptibile de a influența exercitarea competențelor legale ale Autorității, ele pot fi apreciate ca reprezentând o ingerință în autonomia decizională, organizatorică și funcțională a acesteia, contrar dispozițiilor art. 1 alin. (1^1) din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată, cu modificări și completări, prin Legea nr. 140/2012, cu modificările și completările ulterioare. În acest context, se impune reconsiderarea textelor menționate, în vederea asigurării conformității cu statutul de independență al ANCOM. În acest sens, propunem următoarele:

a) completarea textului art. 1 alin. (5) în sensul excluderii din sfera subiectului propunerii legislative acele entități publice ale căror atribuții ar fi afectate de aplicarea noilor norme: *„Prezenta lege se aplică autorităților și instituțiilor publice centrale și locale precum și entităților aflate în subordinea, în administrarea, sub autoritatea, coordonarea sau controlul acestora, cu excepția situațiilor în care, potrivit unor*

[8] Potrivit art. 3 din Ordonanța de urgență a Guvernului nr. 22/2009 privind înființarea Autorității Naționale pentru Administrare și Reglementare în Comunicații, aprobată prin Legea nr. 113/2010, cu modificările și completările ulterioare.

[9] Art. 1 alin. (1) din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată, cu modificări și completări, prin Legea nr. 140/2012, cu modificările și completările ulterioare.

dispoziții legale speciale, aplicarea prezentei legi ar aduce atingere exercitării atribuțiilor legale conferite acestora."

b) completarea textului art. 1 alin. (7) în sensul excluderii din sfera obiectului propunerii legislative a acelor resurse digitale publice care pot afecta exercitarea atribuțiilor legale: *„Prezenta lege nu se aplică sistemelor informatice și de comunicații care vehiculează informații clasificate, potrivit legii, precum și acelor resurse digitale publice care sunt utilizate exclusiv pentru exercitarea unor atribuții legale a căror natură este incompatibilă cu obiectivul prezentei legi prevăzut la alin. (4)."*

Cu stimă,

Președinte,

Valeriu Ștefan ZGONEA