



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

Numărul notificării : 2026/0346/ES (Spain)

Proiect de decret regal privind securitatea și reziliența rețelelor și serviciilor de comunicații electronice, precum și a anumitor infrastructuri digitale

Data primirii : 08/07/2026

Terminarea perioadei de status quo : 09/10/2026

Message

Mesaj 001

Comunicarea Comisiei - TRIS/(2026) 1822

Directiva (UE) 2015/1535

Notificare: 2026/0346/ES

Notificarea unui proiect de text din partea unui stat membru

Notification – Notificación – Notifizierung – Нотификация – Oznámení – Notifikation – Γνωστοποίηση – Notificación – Teavitamine – Ilmoitus – Obavijest – Bejelentés – Notifica – Pranešimas – Paziņojums – Notifika – Kennisgeving – Zawiadomienie – Notificação – Notificare – Oznámenie – Obvestilo – Anmälan – Fógra a thabhairt

Does not open the delays - N'ouvre pas de délai - Kein Fristbeginn - Не се предвижда период на прекъсване - Nezahajuje prodlení - Fristerne indledes ikke - Καμμία έναρξη προθεσμίας - No abre el plazo - Viivituste perioodi ei avata - Määräaika ei ala tästä - Ne otvara razdoblje kašnjenja - Nem nyitja meg a késéset - Non fa decorrere la mora - Atidējimai nepradedami - Atlikšanas laikposms nesākas - Ma jiftaħ il-perijodi ta' dewmien - Geen termijnbegin - Nie otwiera opóźnień - Não inicia o prazo - Nu deschide perioadele de stagnare - Nezačína oneskorenia - Ne uvaja zamud - Inleder ingen frist - Ní osclaíonn sé na moilleanna

MSG: 20261822.RO

1. MSG 001 IND 2026 0346 ES RO 08-07-2026 ES NOTIF

2. Spain

3A. Subdirección General de Ordenación de las Telecomunicaciones.

Secretaría General de Telecomunicaciones, Infraestructuras Digitales y Seguridad Digital.

Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

Ministerio para la Transformación Digital y de la Función Pública

Calle Poeta Joan Maragall 41

28020 Madrid

+34 913462750

3B. Subdirección General de Ordenación de las Telecomunicaciones.

Secretaría General de Telecomunicaciones, Infraestructuras Digitales y Seguridad Digital.

Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

Ministerio para la Transformación Digital y de la Función Pública



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

Calle Poeta Joan Maragall 41
28020 Madrid
+34 913462750

4. 2026/0346/ES - V00T - Telecomunicații

5. Proiect de decret regal privind securitatea și reziliența rețelelor și serviciilor de comunicații electronice, precum și a anumitor infrastructuri digitale

6. Scopul proiectului este de a consolida securitatea, reziliența și continuitatea rețelelor și a serviciilor de comunicații electronice, a instalațiilor asociate acestora și a anumitor infrastructuri digitale în Spania.

7.

8. Proiectul de decret regal urmărește să asigure securitatea, reziliența și continuitatea rețelelor și serviciilor de comunicații electronice, a resurselor asociate acestora și a anumitor infrastructuri digitale din Spania.

Obiectivul este de a asigura furnizarea de servicii esențiale în caz de incidente de securitate, întreruperi ale serviciilor sau degradări semnificative, precum și de a reglementa obligațiile de raportare a unor astfel de incidente autorităților competente.

Obligațiile prevăzute de decret se aplică operatorilor de rețele publice de comunicații electronice, furnizorilor de servicii de comunicații electronice destinate publicului, administratorilor de resurse asociate și operatorilor anumitor infrastructuri digitale, precum cablurile submarine, sistemele prin satelit, centrele de prelucrare a datelor (CPD), rețelele de distribuție a conținutului (CDN) și punctele de schimb de trafic internet (IXP), precum și, în anumite privințe, centrelor de preluare a apelurilor de urgență 112 și sistemelor de alertă publică. Se recunoaște, de asemenea, rolul esențial al acestor rețele și infrastructuri în situații de urgență.

Se prevede elaborarea unui „Plan național de securitate și reziliență”, care va defini organizarea răspunsului în situații de criză și mecanismele de coordonare instituțională. De asemenea, se instituie obligația entităților vizate de a elabora un „plan general”, aplicabil fiecărei entități obligate, precum și „planuri specifice” pentru fiecare tip de rețea și serviciu. Aceste planuri trebuie să includă analize de risc, identificarea infrastructurilor esențiale, măsuri preventive, mecanisme de redresare și protocoale de intervenție pentru diferite scenarii, precum întreruperile alimentării cu energie electrică, fenomenele naturale, incendiile, defecțiunile informatice sau atacurile cibernetice.

Se introduc obligații specifice pentru a asigura continuitatea serviciilor de telecomunicații. Operatorii trebuie să adopte măsuri pentru a reduce la minimum impactul incidentelor și pentru a garanta funcționarea serviciilor esențiale, în special a comunicațiilor de urgență. În situații excepționale, aceștia pot acorda prioritate anumitor categorii de trafic, precum comunicațiile de urgență sau serviciile de voce și SMS, cu respectarea principiului neutralității tehnologice. În plus, sunt stabilite cerințe minime privind autonomia energetică a infrastructurilor esențiale, iar rețelele mobile au obligația de a asigura, în mod progresiv, o autonomie energetică minimă de patru ore pentru acoperirea, în termen de trei ani, a cel puțin 75 % din populație.

Proiectul instituie un sistem de notificare a incidentelor semnificative care nu sunt considerate incidente de securitate cibernetică, acestea din urmă fiind reglementate de Directiva NIS2 și de Directiva privind reziliența entităților critice (CER). Operatorii notifică Secretariatului de Stat orice incident semnificativ în termen de cel mult o oră de la momentul la care au luat cunoștință de acesta, transmit ulterior actualizări periodice pe durata afectării serviciului și prezintă un raport final după restabilirea acestuia.

Sunt stabilite măsuri specifice privind comunicațiile de urgență prin intermediul numărului unic european de urgență 112 și al sistemelor de alertă publică. Atât centrele de preluare a apelurilor de urgență, cât și operatorii, trebuie să implementeze măsuri de redundanță și de asigurare a continuității serviciilor, să elaboreze planuri specifice de intervenție și să notifice imediat orice întrerupere a acestor servicii, astfel de întreruperi fiind considerate automat incidente semnificative.

Decretul regal completează măsurile și mecanismele de coordonare prevăzute de cadrul normativ privind securitatea cibernetică și reziliența entităților critice (Directiva NIS2 și Directiva CER), prin instituirea unui Comitet de coordonare pentru securitate și reziliență, precum și prin dezvoltarea ulterioară a unor platforme electronice destinate gestionării și



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

notificării incidentelor. În ansamblu, decretul reprezintă o consolidare semnificativă a obligațiilor privind securitatea, continuitatea serviciilor și supravegherea aplicabile sectorului comunicațiilor electronice și infrastructurilor digitale critice.

9. Digitalizarea tot mai accentuată a economiei și a serviciilor publice a condus la o creștere semnificativă a dependenței de rețelele de comunicații electronice și de infrastructurile digitale care le susțin funcționarea. Această situație a evidențiat existența unor vulnerabilități și riscuri care nu se limitează exclusiv la domeniul securității cibernetice, ci afectează și securitatea fizică, precum și capacitatea infrastructurilor de a rezista și de a se redresa în urma unor evenimente perturbatoare. În acest context, regulamentul consideră că este necesară consolidarea capacității de prevenire, reacție și redresare în cazul unor incidente care ar putea compromite disponibilitatea, integritatea sau funcționarea rețelilor și serviciilor de comunicații electronice.

Expunerea de motive a proiectului de decret regal evidențiază o serie de evenimente recente care au demonstrat necesitatea consolidării rezilienței acestor infrastructuri. Printre acestea se numără fenomene naturale, cum ar fi erupția vulcanică din La Palma din 2021 și sistemul de joasă presiune rece care a afectat diferite părți ale Spaniei în 2024, precum și incidente de origine nenaturală, cum ar fi recenta întrerupere a alimentării cu energie electrică la nivel național. Aceste evenimente au demonstrat că, atât fenomenele naturale extreme, cât și defectiunile tehnice sau întreruperile alimentării cu energie pot provoca perturbări semnificative ale rețelilor de comunicații și pot pune în pericol continuitatea furnizării unor servicii esențiale pentru cetățeni și autoritățile publice.

În plus, transformarea digitală modifică profund arhitectura și funcționarea rețelilor de telecomunicații. Încorporarea unor tehnologii precum internetul obiectelor (IoT), inteligența artificială (IA), volumele mari de date, cloud computing și virtualizarea serviciilor a făcut posibilă îmbunătățirea eficienței, a conectivității și a dezvoltării economice, dar, în același timp, a mărit complexitatea sistemelor și a generat noi riscuri operaționale și de securitate. Prin urmare, consideră că este esențial ca acest cadru de reglementare să evolueze pentru a anticipa aceste riscuri și pentru a asigura niveluri adecvate de protecție și reziliență.

Din punct de vedere juridic, inițiativa se întemeiază în principal pe articolul 63 din Legea nr. 11/2022 privind comunicațiile, referitor la integritatea și securitatea rețelilor și serviciilor de comunicații electronice. În plus, aceasta se bazează pe legislația existentă privind securitatea rețelilor 5G, în special pe Decretul-lege regal nr. 7/2022, pe Decretul-lege regal nr. 12/2018 privind securitatea rețelilor și a sistemelor informatice, precum și pe Decretul regal nr. 443/2024 de aprobare a Cadrului național de securitate pentru rețelele și serviciile 5G. Fără a aduce atingere acestor acte normative, deși ele au reprezentat progrese importante, este necesară instituirea unui cadru specific care să abordeze în mod cuprinzător securitatea și reziliența ansamblului rețelilor și serviciilor de comunicații electronice și ale anumitor infrastructuri digitale.

În cele din urmă, textul explică faptul că noul decret regal urmărește să acționeze în mod complementar față de viitoarea legislație spaniolă privind securitatea cibernetică și reziliența entităților critice. În consecință, obligațiile care decurg din reglementările de transpunere a NIS2 și CER vor continua să se aplice în întregime incidentelor de securitate cibernetică, precum și incidentelor care afectează rețelele, serviciile și infrastructurile digitale și care nu sunt reglementate în mod expres în prezentul decret regal. În acest mod, se urmărește asigurarea coerenței dintre diferitele instrumente normative, evitarea suprapunerilor de reglementare și instituirea unui sistem integrat de protecție care să consolideze securitatea, continuitatea și reziliența comunicațiilor electronice și a infrastructurilor digitale esențiale pentru funcționarea societății și economiei spaniole.

9a. Măsura este adecvată pentru atingerea obiectivului urmărit, și anume consolidarea securității, a rezilienței și a continuității rețelilor și serviciilor de comunicații electronice, precum și a anumitor infrastructuri digitale.

Experiența dobândită în ultimii ani a arătat că rețelele de telecomunicații sunt infrastructuri esențiale pentru funcționarea societății, astfel cum s-a demonstrat în timpul pandemiei de COVID-19, precum și în situații de urgență generate de evenimente naturale extreme, de întreruperi ale alimentării cu energie electrică sau de incidente de securitate care au afectat disponibilitatea serviciilor. În acest context, adoptarea unui cadru de reglementare specific reprezintă un mijloc adecvat pentru consolidarea capacității de prevenire, răspuns și redresare în cazul incidentelor care pot compromite continuitatea comunicațiilor electronice.

Regulamentul pune în aplicare dispozițiile prevăzute la articolul 63 din Legea nr. 11/2022, Legea generală privind telecomunicațiile. De asemenea, acesta completează și adaptează cadrul de reglementare la evoluțiile tehnologice și la noile riscuri asociate digitalizării, virtualizării rețelilor, cloud computing-ului, inteligenței artificiale și internetului obiectelor (IoT), a căror adoptare tot mai largă sporește expunerea la vulnerabilități atât de natură fizică, cât și digitală.



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

În acest sens, decretul regal este instrumentul adecvat pentru specificarea obligațiilor sectoriale care permit o abordare cuprinzătoare a particularităților tehnice și operaționale ale sectorului telecomunicațiilor.

Caracterul adecvat al măsurii se reflectă în special în integrarea unor mecanisme preventive și de planificare menite să îmbunătățească gradul de pregătire al operatorilor în situații de criză. Obligația de a elabora „planuri generale” și „planuri specifice” pentru fiecare rețea sau serviciu, precum și elaborarea unui „Plan național de securitate și reziliență” și a unui „Plan național de urgență civilă”, permite stabilirea unor proceduri specifice pentru identificarea riscurilor, prevenirea acestora, intervenția în caz de urgență și redresarea.

De asemenea, actualizarea procedurilor de notificare a incidentelor constituie o măsură adecvată pentru îmbunătățirea capacității autorităților competente de supraveghere și gestionare a situațiilor de criză. Experiența acumulată a demonstrat necesitatea adaptării criteriilor, termenelor și conținutului notificărilor la o realitate tehnologică și operațională din ce în ce mai complexă.

Totodată, măsura este adecvată pentru consolidarea protecției serviciilor deosebit de sensibile, precum comunicațiile de urgență prin intermediul numărului unic european de urgență 112 și sistemele de alertă publică, prin impunerea unor obligații specifice privind continuitatea serviciilor, redundanța și notificarea incidentelor atât operatorilor, cât și centrelor de preluare a apelurilor de urgență. Aceasta contribuie la garantarea continuității furnizării acestor servicii critice chiar și în situații de afectare gravă a infrastructurilor de comunicații.

Instituirea unor mecanisme de cooperare între administrațiile publice, autoritățile naționale și cele europene, precum și constituirea unui comitet permanent de coordonare cu participarea diferitelor părți implicate reprezintă un instrument adecvat pentru facilitarea schimbului de informații, consolidarea coordonării instituționale și promovarea bunelor practici în materie de securitate și reziliență.

În cele din urmă, măsura este în concordanță cu cadrul de reglementare european derivat din directivele NIS2 și CER, asigurând o coordonare adecvată cu viitoarea legislație națională de transpunere și prevenind lacunele de reglementare într-un sector strategic pentru economie și securitatea națională.

9b. Adoptarea decretului regal răspunde unei nevoi reale și dovedite de consolidare a capacității de prevenire, protecție și recuperare a infrastructurilor care au devenit esențiale pentru funcționarea societății, a economiei și a serviciilor publice.

Digitalizarea tot mai accentuată a activităților economice și sociale, împreună cu dependența din ce în ce mai mare de rețelele și serviciile de comunicații electronice, precum și evenimente precum erupția vulcanică din La Palma, fenomenul meteorologic DANA care a afectat diferite regiuni ale teritoriului național sau recenta pană generalizată de energie electrică au demonstrat că rețelele și serviciile de comunicații electronice sunt expuse unor riscuri de natură foarte diversă, care pot compromite în mod grav furnizarea serviciilor esențiale destinate cetățenilor, întreprinderilor și autorităților publice. Aceste evenimente au evidențiat necesitatea consolidării rezilienței infrastructurilor digitale și a îmbunătățirii capacității de răspuns în situații de urgență și de criză.

Această măsură este necesară pentru a pune în aplicare articolul 63 din Legea nr. 11/2022, Legea generală privind telecomunicațiile, care prevede obligația operatorilor de a gestiona riscurile de securitate în mod corespunzător și de a asigura integritatea rețelelor și a serviciilor lor. Este esențial să se elaboreze reglementări care să precizeze mai detaliat obligațiile privind planificarea, prevenirea, raportarea incidentelor, coordonarea instituțională și supravegherea pe care operatorii și celelalte părți implicate trebuie să le îndeplinească.

De asemenea, necesitatea reglementării este justificată de caracterul parțial depășit al cadrului de reglementare aflat în prezent în vigoare în ceea ce privește notificarea incidentelor. Procedurile existente nu mai răspund în mod adecvat complexității incidentelor care pot afecta în prezent rețelele, serviciile și infrastructurile digitale. Actualizarea categoriilor de incidente, a procedurilor de notificare și a termenelor de raportare este necesară pentru ca autoritățile competente să dispună de informații suficiente și actualizate, care să permită coordonarea unui răspuns rapid și eficient în situații de criză.

Totodată, este necesară instituirea unor mecanisme specifice pentru asigurarea continuității unor servicii de importanță deosebită, precum comunicațiile de urgență prin intermediul numărului unic european de urgență 112 și sistemele de alertă publică. Experiența demonstrează că orice întrerupere a acestor servicii poate avea consecințe directe asupra protecției vieții, integrității fizice a persoanelor și gestionării situațiilor de urgență. În consecință, regulamentul impune obligații specifice în ceea ce privește planificarea, redundanța și continuitatea operațională atât pentru operatori, cât și pentru centrele de apel de urgență.

Pe de altă parte, măsura este necesară pentru îmbunătățirea mecanismelor de cooperare la nivel național și european,



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

prin instituirea unui comitet specific de coordonare care să faciliteze schimbul de informații, partajarea experienței și stabilirea unor proceduri comune de intervenție în cazul incidentelor care, prin natura lor, afectează simultan mai mulți operatori și mai multe infrastructuri.

În cele din urmă, este necesar să se asigure coerența sistemului juridic spaniol cu noul cadru european de reglementare derivat din Directiva NIS2 și din Directiva REC. Aceste directive consolidează obligațiile privind securitatea, gestionarea riscurilor și reziliența infrastructurilor critice și impun statelor membre instituirea unor mecanisme eficiente de prevenire, detectare, răspuns și redresare în cazul incidentelor.

9c. Măsura propusă nu impune o sarcină excesivă sau disproporționată în raport cu obiectivele urmărite, deoarece obligațiile pe care le introduce răspund necesității de a asigura securitatea, reziliența și continuitatea infrastructurilor care sunt esențiale pentru funcționarea societății, a economiei și a serviciilor publice.

Proportionalitatea măsurii reiese, în primul rând, din faptul că multe dintre obligațiile prevăzute fac deja parte din practicile standard de gestionare a riscurilor și de asigurare a continuității activității ale operatorilor de telecomunicații și ale administratorilor de infrastructură digitală. Analizele de risc, planurile de urgență, protocoalele de recuperare și mecanismele de supraveghere sunt elemente standard în gestionarea infrastructurii critice și a serviciilor esențiale. Decretul regal nu impune crearea unor structuri complet noi, ci mai degrabă sistematizează și omogenizează anumite obligații pentru a asigura standarde minime comune tuturor entităților obligate.

De asemenea, măsurile prevăzute sunt adecvate în raport cu amploarea riscurilor pe care urmăresc să le atenueze. Având în vedere aceste riscuri, obligația de a dispune de planuri de securitate și reziliență, de mecanisme de rezervă și de proceduri de notificare timpurie constituie un răspuns rezonabil și necesar pentru limitarea efectelor negative și accelerarea restabilirii serviciilor.

Regulamentul include, de asemenea, mecanisme care permit adaptarea obligațiilor la circumstanțele fiecărei entități reglementate. Planurile specifice trebuie elaborate ținând seama de caracteristicile fiecărei rețele, fiecărui serviciu sau fiecărei infrastructuri, permițând operatorilor să stabilească măsurile tehnice și organizatorice cele mai adecvate în funcție de riscurile specifice cu care se confruntă. Această flexibilitate evită impunerea unor soluții uniforme sau rigide care ar putea genera costuri inutile și favorizează o abordare bazată pe gestionarea eficientă a riscurilor.

În ceea ce privește notificarea incidentelor, obligațiile instituite sunt justificate de necesitatea de a dispune de informații actualizate și fiabile care să permită coordonarea răspunsului la incidente ce pot afecta un număr mare de utilizatori, operatori sau teritorii. În plus, informațiile solicitate sunt aceleași pe care operatorii trebuie deja să le colecteze și să le gestioneze în cadrul propriilor proceduri interne pentru soluționarea incidentelor și asigurarea continuității serviciilor lor, astfel încât acestea nu reprezintă o sarcină administrativă disproporționată în raport cu beneficiile generate în ceea ce privește coordonarea și capacitatea de răspuns.

Raportul de evaluare a impactului normativ concluzionează, de asemenea, că impactul economic care rezultă din regulament este gestionabil și proporțional cu interesul public pe care îl protejează. Deși costul financiar estimat pentru entitățile reglementate este cuprins între 45 de milioane EUR și 90 de milioane EUR, acest cost este legat în principal de investițiile care vizează consolidarea rezilienței infrastructurii și asigurarea continuității serviciilor esențiale. În plus, noile sarcini administrative sunt estimate la aproximativ 19 276 EUR, o sumă redusă în comparație cu volumul de activitate și cu dimensiunea economică a operatorilor în cauză. În plus, regulamentul nu implică costuri bugetare pentru autoritățile publice și nici nu are un impact semnificativ asupra concurenței.

Considerând toate aceste motive, se poate concluziona că măsura nu impune sarcini excesive părților care fac obiectul acesteia, ci stabilește mai degrabă obligații care sunt proporționale, rezonabile și necesare pentru a asigura un nivel ridicat de securitate și reziliență a rețelelor și serviciilor de comunicații electronice.

10. Trimiteri la textele de bază:

11. Nu

12.

13. Da

Interesele strategice ale țării

Rețelele și serviciile de comunicații electronice sunt infrastructuri esențiale pentru securitatea națională, serviciile



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

publice, serviciile de urgență, activitatea economică și coeziunea teritorială.

14. Nu

15. Da

16.

Aspect TBT: Nu

Aspect SPS: Nu

Comisiei Europene

Punct de contact pentru Directiva (UE) 2015/1535

email: grow-dir2015-1535-central@ec.europa.eu