



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

Single Market Enforcement

Notification of Regulatory Barriers

Číslo oznámenia : 2026/0346/ES (Spain)

Návrh kráľovského dekrétu o bezpečnosti a odolnosti elektronických komunikačných sietí a služieb a určitých digitálnych infraštruktúr.

Dátum doručenia : 08/07/2026

Koniec zastavenia konania : 09/10/2026

Message

Správa 001

Oznámenie (správa) komisie- TRIS/(2026) 1822

smernica (EÚ) 2015/1535

Oznámenie: 2026/0346/ES

Oznámenie návrhu znenia od členského štátu

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 - Καμία 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.SK

1. MSG 001 IND 2026 0346 ES SK 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

Calle Poeta Joan Maragall 41

28020 Madrid



EUROPEAN COMMISSION

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

+34 913462750

4. 2026/0346/ES - V00T - Telekomunikácie

5. Návrh kráľovského dekrétu o bezpečnosti a odolnosti elektronických komunikačných sietí a služieb a určitých digitálnych infraštruktúr.

6. Jeho cieľom je posilniť bezpečnosť, odolnosť a kontinuitu elektronických komunikačných sietí a služieb, ich súvisiacich zariadení a určitých digitálnych infraštruktúr v Španielsku.

7.

8. Cieľom kráľovského dekrétu je zabezpečiť bezpečnosť, odolnosť a kontinuitu elektronických komunikačných sietí a služieb, ich súvisiacich zariadení a určitých digitálnych infraštruktúr v Španielsku.

Cieľom je zabezpečiť poskytovanie základných služieb v prípade bezpečnostných incidentov, prerušenia služieb alebo ich výrazného zhoršenia, ako aj upraviť povinnosti týkajúce sa oznamovania takýchto incidentov príslušným orgánom.

Povinnými subjektmi sú prevádzkovatelia verejných elektronických komunikačných sietí, poskytovatelia verejne dostupných služieb, prevádzkovatelia súvisiacich zariadení a digitálnych infraštruktúr, ako sú podmorské káble, satelitné systémy, centrá na spracovanie údajov (DPC), siete na sprístupňovanie obsahu (CDN) a internetové prepojujacie uzly (IXP), ako aj v určitých ohľadoch centrá tiesňového volania 112 a systémy varovania verejnosti. Uznáva sa tiež nevyhnutná povaha týchto sietí a infraštruktúr v núdzových situáciách.

Vypracúva sa „Národný plán bezpečnosti a odolnosti“, v ktorom sa stanovuje organizácia reakcie na krízu a mechanizmy inštitucionálnej koordinácie. Zároveň sa v ňom stanovuje povinnosť pre povinné subjekty vypracovať „Všeobecný plán“ pre každý povinný subjekt a „Špecifické plány“ pre každý typ siete a špecifické služby. Musia obsahovať analýzy rizík, identifikáciu základnej infraštruktúry, preventívne opatrenia, mechanizmy obnovy a akčné protokoly pre rôzne scenáre, ako sú výpadky elektrickej energie, prírodné katastrofy, požiare, poruchy IT systémov alebo kybernetické útoky.

Zavádzajú sa špecifické povinnosti na zabezpečenie kontinuity telekomunikačných služieb. Prevádzkovatelia musia prijať opatrenia na minimalizáciu vplyvu incidentov a na zabezpečenie fungovania základných služieb, najmä núdzovej komunikácie. Za výnimočných okolností môžu uprednostniť určité druhy prevádzky, ako sú tiesňové komunikácie alebo hlasové služby a služby SMS, pričom vždy dodržiavajú zásadu technologickej neutrality. Okrem toho sa pre základnú infraštruktúru stanovujú minimálne požiadavky na energetickú autonómiu a mobilným sieťam sa ukladá povinnosť postupne zabezpečiť minimálne štvorhodinové záložné napájanie pre 75 % obyvateľstva do troch rokov.

Zahŕňa systém oznamovania významných incidentov, ktoré sa nepovažujú za kybernetické bezpečnostné incidenty; tieto incidenty sú upravené v smernici NIS2 a v smernici CER. Prevádzkovatelia musia oznámiť štátnemu sekretariátu akýkoľvek významný incident do jednej hodiny od jeho zistenia a následne musia počas trvania výpadku poskytovať pravidelné aktualizácie a po obnovení služby predložiť záverečnú správu.

Stanovujú sa špecifické opatrenia týkajúce sa tiesňovej komunikácie prostredníctvom čísla 112 a systémov varovania verejnosti. Centrá tiesňového volania aj prevádzkovatelia musia zaviesť opatrenia na zabezpečenie redundancie a kontinuity činností, vypracovať konkrétne pohotovostné plány a bezodkladne oznamovať akékoľvek narušenie týchto služieb, ktoré sa automaticky klasifikujú ako významné incidenty.

V kráľovskom dekréte sa stanovujú opatrenia a mechanizmy koordinácie s predpismi o kybernetickej bezpečnosti a odolnosti pre kritické subjekty (smernica NIS2 a smernica CER), zriadenie koordinačného výboru pre bezpečnosť a odolnosť a budúce zavedenie digitálnych platforiem pre riadenie incidentov a komunikáciu. Celkovo ide o výrazné posilnenie povinností v oblasti bezpečnosti, kontinuity a dohľadu, ktoré sa vzťahujú na telekomunikačný sektor a kritické digitálne infraštruktúry.

9. Rastúca digitalizácia hospodárstva a verejných služieb výrazne zvýšila závislosť od elektronických komunikačných sietí a digitálnych infraštruktúr, ktoré ich podporujú. Táto situácia poukázala na existenciu zraniteľností a rizík, ktoré sa neobmedzujú výlučne na oblasť kybernetickej bezpečnosti, ale ovplyvňujú aj fyzickú bezpečnosť a schopnosť infraštruktúr odolávať nepriaznivým udalostiam a zotavovať sa z nich. V tejto súvislosti sa v predpise považuje za potrebné posilniť kapacity na prevenciu, reakciu a obnovu v prípade incidentov, ktoré by mohli ohroziť dostupnosť, integritu alebo



EUROPEAN COMMISSION

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

fungovanie elektronických komunikačných sietí a služieb.

V odôvodnení kráľovského dekrétu sa poukazuje na viacero nedávnych udalostí, ktoré poukázali na potrebu zvýšiť odolnosť týchto infraštruktúr. Medzi nimi sa spomínajú prírodné javy, napríklad sopečná erupcia na ostrove La Palma v roku 2021 a studená tlaková níž spojená so záplavami, ktorá v roku 2024 zasiahla rôzne časti Španielska, ako aj udalosti iného ako prírodného pôvodu, ako napríklad nedávny výpadok elektrickej energie v celej krajine. Tieto udalosti ukázali, že nielen extrémne prírodné javy, ale aj technické poruchy či výpadky dodávok elektrickej energie môžu spôsobiť výrazné narušenie komunikačných sietí a ohroziť kontinuitu základných služieb pre verejnosť a verejné orgány.

Digitálna transformácia okrem toho zásadne mení architektúru a fungovanie telekomunikačných sietí. Začlenenie technológií, ako je internet vecí (IoT), umelá inteligencia (AI), veľké dáta (Big Data), cloud computing a virtualizácia služieb, umožnilo zlepšiť efektívnosť, konektivitu a hospodársky rozvoj, ale zároveň zvýšilo zložitosť systémov a vytvorilo nové prevádzkové a bezpečnostné riziká. Preto sa považuje za nevyhnutné, aby sa regulačný rámec vyvíjal tak, aby predvídal tieto riziká a zabezpečil primeranú úroveň ochrany a odolnosti.

Z právneho hľadiska je iniciatíva založená predovšetkým na článku 63 zákona č. 11/2022, všeobecného zákona o telekomunikáciách, ktorý sa týka integrity a bezpečnosti elektronických komunikačných sietí a služieb. Okrem toho vychádza z existujúcich právnych predpisov týkajúcich sa bezpečnosti sietí 5G, najmä z kráľovského zákonného dekrétu č. 7/2022, kráľovského zákonného dekrétu č. 12/2018 o bezpečnosti sietí a informačných systémov a kráľovského dekrétu č. 443/2024, ktorým sa schvaľuje národný bezpečnostný rámec pre siete a služby 5G. Bez ohľadu na uvedené skutočnosti, hoci tieto predpisy viedli k významnému pokroku, je potrebné vytvoriť osobitný rámec, ktorý komplexne rieši bezpečnosť a odolnosť všetkých elektronických komunikačných sietí a služieb, ako aj určitých digitálnych infraštruktúr. Na záver sa v texte vysvetľuje, že cieľom nového kráľovského dekrétu je doplniť budúcu španielsku legislatívu v oblasti kybernetickej bezpečnosti a odolnosti kritických subjektov. V dôsledku toho sa povinnosti vyplývajúce z predpisov, ktorými sa transponujú smernice NIS2 a CER, budú naďalej v plnej miere vzťahovať na kybernetické bezpečnostné incidenty a na tie incidenty, ktoré majú vplyv na digitálne siete, služby a infraštruktúry a ktoré nie sú výslovne upravené v tomto kráľovskom dekréte. Cieľom je teda zabezpečiť konzistentnosť medzi rôznymi regulačnými nástrojmi, zabrániť prekryvaniu regulačných opatrení a vytvoriť komplexný systém ochrany, ktorým sa posilní bezpečnosť, kontinuita a odolnosť telekomunikačnej a digitálnej infraštruktúry, ktorá je nevyhnutná pre fungovanie španielskej spoločnosti a španielskeho hospodárstva.

9a. Toto opatrenie je vhodné na dosiahnutie sledovaného cieľa, ktorým je posilnenie bezpečnosti, odolnosti a kontinuity elektronických komunikačných sietí a služieb, ako aj určitých digitálnych infraštruktúr.

Skúsenosti získané v posledných rokoch ukázali, že telekomunikačné siete predstavujú základnú infraštruktúru pre fungovanie spoločnosti, ako sa preukázalo počas pandémie COVID-19, ako aj v núdzových situáciách vyplývajúcich z extrémnych prírodných javov, výpadkov elektrickej energie alebo bezpečnostných incidentov, ktoré ovplyvnili dostupnosť služieb. V tejto súvislosti je vhodné prijať osobitný regulačný rámec s cieľom posilniť schopnosť predchádzať incidentom, ktoré by mohli ohroziť kontinuitu elektronických komunikácií, reagovať na ne a obnoviť prevádzku po týchto incidentoch. Týmto predpisom sa vykonávajú ustanovenia uvedené v článku 63 zákona č. 11/2022, všeobecného zákona o telekomunikáciách. Zároveň sa dopĺňa a prispôsobuje regulačný rámec technologickému vývoju a novým rizikám spojeným s digitalizáciou, virtualizáciou sietí, cloud computingom, umelou inteligenciou a internetom vecí (IoT), ktorých čoraz širšie využívanie zvyšuje vystavenie zraniteľnostiam fyzickej aj digitálnej povahy. V tejto súvislosti je kráľovský dekrét vhodným nástrojom na špecifikovanie sektorových povinností, ktoré umožňujú komplexný prístup k technickým a prevádzkovým osobitostiam telekomunikačného sektora.

Vhodnosť tohto opatrenia sa odráža najmä v začlenení preventívnych a plánovacích mechanizmov zameraných na zlepšenie pripravenosti prevádzkovateľov na krízové situácie. Povinnosť vypracovať „Všeobecné plány“ a „Špecifické plány“ pre jednotlivé siete alebo služby, spolu s vypracovaním „Národného plánu bezpečnosti a odolnosti“ a „Národného plánu civilnej obrany“, umožňuje stanoviť špecifické postupy na identifikáciu rizík, prevenciu, reakciu a obnovu. Podobne aj aktualizácia postupov oznamovania incidentov je vhodným opatrením na zlepšenie kapacity príslušných orgánov v oblasti monitorovania a krízového riadenia. Skúsenosti ukázali, že je potrebné prispôsobiť kritériá, lehoty a obsah oznámení zložitejšej technologickej a prevádzkovej realite.

Okrem toho je toto opatrenie vhodné na posilnenie ochrany obzvlášť citlivých služieb, ako je tiesňová komunikácia prostredníctvom čísla 112 a systémy varovania verejnosti, a to tým, že ukladá prevádzkovateľom aj centráam tiesňového volania špecifické povinnosti týkajúce sa kontinuity, redundancie a oznamovania. To pomáha zabezpečiť udržiavanie týchto kritických služieb aj v situáciách, keď je komunikačná infraštruktúra vážne narušená.



EUROPEAN COMMISSION

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

Vytvorenie mechanizmov spolupráce medzi verejnými orgánmi a vnútroštátnymi a európskymi orgánmi, ako aj zriadenie stáleho koordinačného výboru, do ktorého budú zapojené rôzne zainteresované strany, predstavuje vhodný prostriedok na podporu výmeny informácií, inštitucionálnej koordinácie a zavádzania osvedčených postupov v oblasti bezpečnosti a odolnosti.

Toto opatrenie je napokon v súlade s európskym regulačným rámcom vyplývajúcim zo smerníc NIS2 a CER, čím sa zabezpečuje riadna koordinácia s budúcimi vnútroštátnymi transpozičnými právnymi predpismi a predchádza sa vzniku medzier v regulácii v odvetví, ktoré má strategický význam pre hospodárstvo a národnú bezpečnosť.

9b. Prijatie kráľovského dekrétu je reakciou na skutočnú a preukázanú potrebu posilniť kapacity v oblasti prevencie, ochrany a obnovy infraštruktúr, ktoré sa stali nevyhnutnými pre fungovanie spoločnosti, hospodárstva a verejných služieb.

Rastúca digitalizácia hospodárskych a spoločenských činností v spojení s čoraz väčšou závislosťou od elektronických komunikačných sietí a služieb, ako aj udalosti, ako napríklad sopečná erupcia na ostrove La Palma, studená tlaková níž spojená so záplavami, ktorá zasiahla rôzne časti krajiny, či nedávny výpadok elektrickej energie, ukázali, že elektronické komunikačné siete a služby sú vystavené širokej škále rizík, ktoré by mohli vážne ohroziť poskytovanie základných služieb občanom, podnikom a verejným orgánom. Tieto incidenty zdôraznili potrebu posilniť odolnosť digitálnej infraštruktúry a zlepšiť schopnosť reagovať na núdzové situácie a krízy.

Toto opatrenie je potrebné na vykonávanie a uplatňovanie článku 63 zákona č. 11/2022, všeobecného zákona o telekomunikáciách, v ktorom sa stanovuje povinnosť prevádzkovateľov primerane riadiť bezpečnostné riziká a zabezpečiť integritu svojich sietí a služieb. Je nevyhnutné vypracovať predpisy, v ktorých sa podrobnejšie stanovujú povinnosti týkajúce sa plánovania, prevencie, oznamovania incidentov, inštitucionálnej koordinácie a dohľadu, ktoré musia spĺňať prevádzkovatelia a iné príslušné strany.

Potrebu tejto regulácie odôvodňuje aj čiastočná zastaranosť platného regulačného rámca pre oznamovanie incidentov. Súčasné postupy už nedokážu primerane reagovať na zložitosť incidentov, ktoré môžu v súčasnosti ovplyvniť digitálne siete, služby a infraštruktúry. Aktualizácia typov incidentov, komunikačných postupov a lehôt na podávanie oznámení je nevyhnutná na to, aby príslušné orgány disponovali dostatočnými a aktuálnymi informáciami potrebnými na koordináciu rýchlej a účinnej reakcie na krízové situácie.

Takisto je potrebné vytvoriť špecifické mechanizmy na zabezpečenie kontinuity mimoriadne kritických služieb, ako je tiesňová komunikácia prostredníctvom čísla 112 a systémy varovania verejnosti. Skúsenosti ukazujú, že akékoľvek prerušenie týchto služieb môže mať priame dôsledky na ochranu života, fyzickú integritu osôb a riadenie núdzových situácií. Tento predpis preto ukladá prevádzkovateľom aj centráam tiesňového volania špecifické povinnosti týkajúce sa plánovania, redundancie a kontinuity prevádzky.

Okrem toho je toto opatrenie potrebné na zlepšenie mechanizmov vnútroštátnej a európskej spolupráce a na zriadenie špecializovaného koordinačného výboru, ktorý bude uľahčovať výmenu informácií, zdieľanie skúseností a zavádzanie spoločných postupov pri reagovaní na incidenty, ktoré vzhľadom na svoju povahu zvyčajne postihujú viacerých prevádzkovateľov a infraštruktúru súčasne.

Nakoniec je potrebné zabezpečiť súlad španielskeho právneho systému s novým európskym regulačným rámcom vyplývajúcim zo smerníc NIS2 a CER. Týmto európskymi nástrojmi sa posilňujú povinnosti týkajúce sa bezpečnosti, riadenia rizík a odolnosti kritickej infraštruktúry a od členských štátov sa vyžaduje, aby vytvorili účinné mechanizmy na predchádzanie incidentom, ich odhaľovanie, reakciu na ne a obnovu po nich.

9c. Navrhované opatrenie nepredstavuje nadmerné alebo neprimerané zaťaženie vo vzťahu k sledovaným cieľom, keďže povinnosti, ktoré sa ním zavádzajú, reagujú na potrebu zaistiť bezpečnosť, odolnosť a kontinuitu infraštruktúr, ktoré sú nevyhnutné pre fungovanie spoločnosti, hospodárstva a verejných služieb.

Proporcionálnosť opatrenia je zrejmá predovšetkým zo skutočnosti, že mnohé zo stanovených povinností sú už súčasťou štandardných postupov riadenia rizík a kontinuity činností telekomunikačných operátorov a správcov digitálnej infraštruktúry. Analýzy rizík, pohotovostné plány, protokoly obnovy a mechanizmy dohľadu sú štandardnými prvkami riadenia kritickej infraštruktúry a základných služieb. Kráľovský dekrét neukladá vytvorenie úplne nových štruktúr, ale skôr systematizuje a zjednocuje určité povinnosti s cieľom zabezpečiť minimálne štandardy spoločné pre všetky povinné subjekty.

Okrem toho sú navrhované opatrenia primerané rozsahu rizík, ktoré majú zmierniť. Vzhľadom na tieto riziká je požiadavka mať zavedené plány bezpečnosti a odolnosti, záložné mechanizmy a postupy včasného oznamovania



EUROPEAN COMMISSION

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

primeranou a nevyhnutnou reakciou s cieľom minimalizovať škody a urýchliť obnovu služieb.

Tento predpis tiež obsahuje mechanizmy, ktoré umožňujú prispôsobiť povinnosti okolnostiam každého povinného subjektu. Špecifické plány by mali byť vypracované so zreteľom na charakteristiky každej siete, služby alebo infraštruktúry, aby prevádzkovatelia mohli určiť najvhodnejšie technické a organizačné opatrenia v závislosti od ich špecifických rizík. Touto flexibilitou sa predchádza zavádzaniu jednotných alebo nepružných riešení, ktoré by mohli viesť k zbytočným nákladom, a uprednostňuje sa prístup založený na účinnom riadení rizík.

Pokiaľ ide o oznamovanie incidentov, tieto povinnosti sú odôvodnené potrebou disponovať aktuálnymi a spoľahlivými informáciami na koordináciu reakcie na incidenty, ktoré môžu ovplyvniť veľký počet používateľov, prevádzkovateľov alebo území. Okrem toho ide o informácie, ktoré prevádzkovatelia už teraz musia zhromažďovať a spravovať interne s cieľom riešiť incidenty a zabezpečiť kontinuitu svojich služieb, takže nepredstavujú neprimerané administratívne zaťaženie v porovnaní s prínosmi, ktoré to prináša z hľadiska koordinácie a schopnosti reagovať.

Správa o posúdení vplyvu regulácie tiež konštatuje, že ekonomický vplyv vyplývajúci z tohto predpisu je zvládnuiteľný a primeraný verejnému záujmu, ktorý chráni. Hoci sa odhadované finančné náklady pre povinné subjekty pohybujú v rozmedzí od 45 miliónov EUR do 90 miliónov EUR, tieto náklady súvisia predovšetkým s investíciami zameranými na posilnenie odolnosti infraštruktúry a zabezpečenie kontinuity základných služieb. Okrem toho sa nové administratívne zaťaženie odhaduje na približne 19 276 EUR, čo je nízka suma v porovnaní s rozsahom činnosti a ekonomickou veľkosťou dotknutých prevádzkovateľov. Tento predpis navyše nespôsobuje verejným orgánom žiadne rozpočtové náklady a nemá ani žiadny významný vplyv na hospodársku súťaž.

Na základe všetkých týchto dôvodov možno dospieť k záveru, že opatrenie nepredstavuje nadmerné zaťaženie pre strany, na ktoré sa vzťahuje, ale skôr stanovuje povinnosti, ktoré sú primerané, rozumné a nevyhnutné na zabezpečenie vysokej úrovne bezpečnosti a odolnosti elektronických komunikačných sietí a služieb.

10. Odkazy na základné texty:

11. Nie

12.

13. Áno

Strategické záujmy krajiny

Elektronické komunikačné siete a služby sú základnou infraštruktúrou pre národnú bezpečnosť, verejné služby, záchranné služby, hospodársku činnosť a územnú súdržnosť.

14. Nie

15. Áno

16.

Aspekt technických prekážok obchodu: Nie

Aspekt sanitárnych a
rastlinolekárych opatrení: Nie

Európska komisia

Kontaktný bod smernice (EÚ) 2015/1535

e-mail: grow-dir2015-1535-central@ec.europa.eu