



EUROPEAN COMMISSION

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

Single Market Enforcement

Notification of Regulatory Barriers

Numéro de notification : 2026/0346/ES (Spain)

Projet de décret royal relatif à la sécurité et à la résilience des réseaux et services de communications électroniques et de certaines infrastructures numériques.

Date de réception : 08/07/2026

Fin de la période de statu quo : 09/10/2026

Message

Message 001

Communication de la Commission - TRIS/(2026) 1822

Directive (UE) 2015/1535

Notification: 2026/0346/ES

Notification d'un projet de texte d'un État membre

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.FR

1. MSG 001 IND 2026 0346 ES FR 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 - Télécommunications

5. Projet de décret royal relatif à la sécurité et à la résilience des réseaux et services de communications électroniques et de certaines infrastructures numériques.

6. Elle vise à renforcer la sécurité, la résilience et la continuité des réseaux et services de communications électroniques, des installations qui y sont associées ainsi que de certaines infrastructures numériques en Espagne.

7.

8. Le décret royal vise à assurer la sécurité, la résilience et la continuité des réseaux et services de communications électroniques, de leurs installations associées et de certaines infrastructures numériques en Espagne.

L'objectif est de garantir la fourniture des services essentiels en cas d'incidents de sécurité, d'interruptions de service ou de dégradations importantes, ainsi que de réglementer les obligations de signalement de ces incidents aux autorités.

Les entités assujetties sont les opérateurs de réseaux publics de communications électroniques, les fournisseurs de services accessibles au public, les opérateurs d'installations associées et d'infrastructures numériques telles que les câbles sous-marins, les systèmes satellitaires, les centres de traitement des données (CTD), les réseaux de diffusion de contenu (RDC) et les points d'échange internet (IXP), ainsi que, à certains égards, les centres de traitement des appels d'urgence 112 et les systèmes d'alerte publique. Le rôle essentiel de ces réseaux et infrastructures dans les situations d'urgence est également reconnu.

Un «Plan national de sécurité et de résilience» a été élaboré, qui définira l'organisation de la réponse aux crises ainsi que les mécanismes de coordination institutionnelle. Elle prévoit également l'obligation pour les entités assujetties d'élaborer un «plan général» pour chaque partie assujettie et des «plans spécifiques» pour chaque type de réseau et de services spécifiques. Elles doivent comprendre des analyses des risques, l'identification des infrastructures essentielles, des mesures préventives, des mécanismes de rétablissement et des protocoles d'action pour différents scénarios, tels que des coupures d'électricité, des catastrophes naturelles, des incendies, des défaillances informatiques ou des cyberattaques.

Des obligations spécifiques sont mises en place afin de garantir la continuité des services de télécommunications. Les opérateurs doivent prendre des mesures pour minimiser l'impact des incidents et garantir le bon fonctionnement des services essentiels, en particulier les communications d'urgence. Dans des circonstances exceptionnelles, ils peuvent accorder la priorité à certains types de trafic, tels que les communications d'urgence ou les services vocaux et de SMS, tout en respectant toujours le principe de neutralité technologique. En outre, des exigences minimales en matière d'autonomie énergétique sont fixées pour les infrastructures essentielles, et les réseaux mobiles sont tenus de garantir progressivement, d'ici trois ans, une autonomie d'alimentation de secours d'au moins quatre heures pour 75 % de la population.

Il comprend un système de notification des incidents significatifs qui ne sont pas considérés comme des incidents de cybersécurité, ces derniers étant régis par la directive SRI 2 et la directive CER. Les opérateurs notifient au Secrétariat d'État tout incident significatif dans un délai d'une heure à compter du moment où ils en ont connaissance. Ils fournissent ensuite des mises à jour régulières pendant toute la durée de la perturbation, suivies d'un rapport final une fois le service rétabli.

Des mesures spécifiques sont mises en place pour les communications d'urgence par l'intermédiaire du numéro 112 et des systèmes d'alerte publique. Les centres de traitement des appels d'urgence et les opérateurs doivent mettre en place des mesures de redondance et de continuité des activités, élaborer des plans d'urgence spécifiques et signaler immédiatement toute perturbation de ces services, qui sont automatiquement classés comme des incidents significatifs. Le décret royal définit les mesures et les mécanismes de coordination avec la réglementation en matière de cybersécurité et de résilience applicable aux entités critiques (la directive SRI 2 et la directive CER), la création d'un comité de coordination de la sécurité et de la résilience, ainsi que le déploiement futur de plateformes numériques



EUROPEAN COMMISSION

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

dédiées à la gestion des incidents et à la communication. Dans l'ensemble, cela constitue un renforcement significatif des obligations en matière de sécurité, de continuité et de surveillance applicables au secteur des télécommunications et aux infrastructures numériques critiques.

9. La numérisation croissante de l'économie et des services publics a considérablement accru la dépendance vis-à-vis des réseaux de communications électroniques et des infrastructures numériques qui les soutiennent. Cette situation a mis en évidence l'existence de vulnérabilités et de risques qui ne se limitent pas exclusivement au domaine de la cybersécurité, mais affectent également la sécurité physique et la capacité des infrastructures à résister et à se rétablir à la suite d'événements défavorables. Dans ce contexte, le règlement estime nécessaire de renforcer les capacités de prévention, de réaction et de rétablissement en cas d'incidents susceptibles de compromettre la disponibilité, l'intégrité ou le fonctionnement des réseaux et services de communications électroniques.

L'exposé des motifs du décret royal met en évidence plusieurs événements récents qui ont démontré la nécessité de renforcer la résilience de ces infrastructures. Parmi ceux-ci, le rapport mentionne des phénomènes naturels tels que l'éruption volcanique survenue à La Palma en 2021 et la dépression froide qui a touché différentes régions d'Espagne en 2024, ainsi que des incidents d'origine non naturelle, comme la récente panne d'électricité à l'échelle nationale. Ces événements ont montré que tant les phénomènes naturels extrêmes que les défaillances techniques ou les coupures d'électricité peuvent entraîner des perturbations importantes des réseaux de communication et compromettre la continuité des services essentiels destinés au public et aux pouvoirs publics.

De plus, la transformation numérique modifie profondément l'architecture et le fonctionnement des réseaux de télécommunications. L'intégration de technologies telles que l'internet des objets (IdO), l'intelligence artificielle (IA), les mégadonnées, l'informatique en nuage et la virtualisation des services a permis d'améliorer l'efficacité, la connectivité et le développement économique, tout en augmentant la complexité des systèmes et en créant de nouveaux risques opérationnels et de sécurité. Par conséquent, il estime qu'il est essentiel que le cadre réglementaire évolue afin d'anticiper ces risques et de garantir des niveaux appropriés de protection et de résilience.

D'un point de vue juridique, cette initiative s'appuie principalement sur l'article 63 de la loi n° 11/2022, relative aux télécommunications, qui porte sur l'intégrité et la sécurité des réseaux et services de communications électroniques. En outre, il s'appuie sur la législation existante en matière de sécurité des réseaux 5G, notamment le décret-loi royal n° 7/2022, le décret-loi royal n° 12/2018 relatif à la sécurité des réseaux et des systèmes d'information, ainsi que le décret royal n° 443/2024 approuvant le cadre national de sécurité pour les réseaux et services 5G. Nonobstant ce qui précède, bien que ces réglementations aient permis de réaliser des progrès significatifs, il est nécessaire d'élaborer un cadre spécifique qui traite de manière exhaustive de la sécurité et de la résilience de l'ensemble des réseaux et services de communications électroniques, ainsi que de certaines infrastructures numériques.

Enfin, le texte précise que le nouveau décret royal vise à venir en complément de la future législation espagnole en matière de cybersécurité et de résilience des entités critiques. Par conséquent, les obligations découlant des règlements transposant les directives SRI 2 et CER continueront de s'appliquer pleinement aux incidents de cybersécurité ainsi qu'aux incidents affectant les réseaux, services et infrastructures numériques qui ne sont pas expressément régis par le présent décret royal. L'objectif est ainsi de garantir la cohérence entre les différents instruments réglementaires, d'éviter les chevauchements réglementaires et d'établir un système de protection global qui renforce la sécurité, la continuité et la résilience des infrastructures de télécommunications et numériques essentielles au fonctionnement de la société et de l'économie espagnoles.

9 bis. La mesure est appropriée pour atteindre l'objectif poursuivi consistant à renforcer la sécurité, la résilience et la continuité des réseaux et services de communications électroniques ainsi que de certaines infrastructures numériques. L'expérience acquise ces dernières années a montré que les réseaux de télécommunications constituent des infrastructures essentielles au bon fonctionnement de la société, comme l'ont démontré la pandémie de COVID-19 ainsi que les situations d'urgence liées à des phénomènes naturels extrêmes, à des coupures d'électricité ou à des incidents de sécurité qui ont affecté la disponibilité des services. Dans ce contexte, l'adoption d'un cadre réglementaire spécifique s'avère appropriée pour renforcer les capacités de prévention, d'intervention et de reprise après sinistre face à des incidents susceptibles de compromettre la continuité des communications électroniques.

Ce règlement met en œuvre les dispositions de l'article 63 de la loi n° 11/2022, relative aux télécommunications. Il complète et adapte également le cadre réglementaire aux évolutions technologiques et aux nouveaux risques liés à la numérisation, à la virtualisation des réseaux, à l'informatique en nuage, à l'intelligence artificielle et à l'Internet des



EUROPEAN COMMISSION

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

objets (IoT), dont l'adoption croissante accroît l'exposition à des vulnérabilités tant physiques que numériques. À cet égard, le décret royal constitue l'instrument approprié pour définir les obligations sectorielles permettant une approche globale des particularités techniques et opérationnelles du secteur des télécommunications.

L'adéquation de la mesure se reflète notamment dans l'intégration de mécanismes de prévention et de planification visant à améliorer la préparation des opérateurs face aux situations de crise. L'obligation d'élaborer des «plans généraux» et des «plans spécifiques» par réseau ou service, ainsi que l'élaboration d'un «plan national de sécurité et de résilience» et d'un «plan national d'urgence civile», permettent d'établir des procédures spécifiques pour l'identification des risques, la prévention, la réaction et la reprise.

De même, la mise à jour des procédures de notification des incidents est une mesure appropriée pour améliorer la capacité de surveillance et de gestion des crises des autorités compétentes. L'expérience a montré qu'il était nécessaire d'adapter les critères, les délais et le contenu des notifications à une réalité technologique et opérationnelle plus complexe.

De plus, cette mesure est bien adaptée pour renforcer la protection des services particulièrement sensibles, tels que les communications d'urgence via le numéro 112 et les systèmes d'alerte publique, en imposant des obligations spécifiques en matière de continuité, de redondance et de notification tant aux opérateurs qu'aux centres de traitement des appels d'urgence. Cela contribue à garantir le maintien de ces services critiques, même dans les situations où les infrastructures de communication sont gravement perturbées.

La mise en place de mécanismes de coopération entre les pouvoirs publics et les autorités nationales et européennes, ainsi que la création d'un comité de coordination permanent réunissant les différentes parties prenantes, constituent des moyens appropriés pour favoriser l'échange d'informations, la coordination institutionnelle et l'adoption des meilleures pratiques dans le domaine de la sécurité et de la résilience.

Enfin, cette mesure s'inscrit dans le cadre réglementaire européen découlant des directives SRI 2 et CER, garantissant ainsi une coordination adéquate avec les futures législations nationales de transposition et évitant tout vide réglementaire dans un secteur stratégique pour l'économie et la sécurité nationale.

9 ter. L'adoption du décret royal répond à un besoin réel et avéré de renforcer les capacités de prévention, de protection et de remise en état des infrastructures devenues indispensables au bon fonctionnement de la société, de l'économie et des services publics.

La numérisation accrue des activités économiques et sociales, associée à une dépendance grandissante aux réseaux et services de communications électroniques, ainsi que des événements tels que l'éruption volcanique à La Palma, la dépression froide qui a touché plusieurs régions du pays, ou la récente panne d'électricité, ont démontré que les réseaux et services de communications électroniques sont exposés à une grande variété de risques susceptibles de compromettre gravement la fourniture de services essentiels aux citoyens, aux entreprises et aux autorités publiques. Ces incidents ont mis en évidence la nécessité de renforcer la résilience des infrastructures numériques et d'améliorer la capacité de réaction aux urgences et aux crises.

Cette mesure est nécessaire pour mettre en œuvre et donner effet à l'article 63 de la loi 11/2022, la loi générale sur les télécommunications, qui prévoit l'obligation pour les opérateurs de gérer les risques de sécurité de manière appropriée et de garantir l'intégrité de leurs réseaux et services. Il est essentiel d'élaborer des règlements qui détaillent les obligations en matière de planification, de prévention, de notification des incidents, de coordination institutionnelle et de surveillance que les opérateurs et les autres parties concernées doivent remplir.

De même, la nécessité de ce règlement se justifie par l'obsolescence partielle du cadre réglementaire actuellement en vigueur en matière de notification des incidents. Les procédures actuelles ne permettent plus de répondre de manière adéquate à la complexité des incidents susceptibles d'affecter aujourd'hui les réseaux, les services et les infrastructures numériques. La mise à jour des types d'incidents, des procédures de communication et des délais de notification est nécessaire pour que les autorités compétentes disposent d'informations suffisantes et à jour leur permettant de coordonner une réponse rapide et efficace face à des situations de crise.

Il est également nécessaire de mettre en place des mécanismes spécifiques pour assurer la continuité des services particulièrement critiques, tels que les communications d'urgence par l'intermédiaire du numéro 112 et les systèmes d'alerte publique. L'expérience montre que toute interruption de ces services peut avoir des conséquences directes sur la protection de la vie, l'intégrité physique des personnes et la gestion des situations d'urgence. Par conséquent, le règlement impose des obligations spécifiques en matière de planification, de redondance et de continuité opérationnelle tant aux opérateurs qu'aux centres de traitement des appels d'urgence.



EUROPEAN COMMISSION

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

En outre, cette mesure est nécessaire pour améliorer les mécanismes de coopération nationaux et européens, et pour mettre en place un comité de coordination dédié, chargé de faciliter l'échange d'informations, le partage d'expériences et l'établissement de procédures communes pour faire face à des incidents qui, de par leur nature même, ont tendance à toucher simultanément plusieurs opérateurs et infrastructures.

Enfin, il est nécessaire de garantir la cohérence du système juridique espagnol avec le nouveau cadre réglementaire européen découlant des directives SRI 2 et CER. Ces instruments européens renforcent les obligations en matière de sécurité, de gestion des risques et de résilience des infrastructures critiques, et exigent des États membres qu'ils mettent en place des mécanismes efficaces de prévention, de détection, de réaction et de rétablissement à la suite d'incidents.

9 quater. La mesure proposée n'impose pas une charge excessive ou disproportionnée par rapport aux objectifs poursuivis, dans la mesure où les obligations qu'elle instaure répondent à la nécessité de garantir la sécurité, la résilience et la continuité des infrastructures essentielles au bon fonctionnement de la société, de l'économie et des services publics.

La proportionnalité de cette mesure ressort avant tout du fait que bon nombre des obligations prévues font déjà partie des pratiques courantes en matière de gestion des risques et de continuité des activités des opérateurs de télécommunications et des gestionnaires d'infrastructures numériques. Les analyses des risques, les plans d'urgence, les protocoles de rétablissement et les mécanismes de surveillance sont des éléments standard de la gestion des infrastructures critiques et des services essentiels. Le décret royal n'impose pas la création de structures entièrement nouvelles, mais vise plutôt à systématiser et à harmoniser certaines obligations afin de garantir des normes minimales communes à toutes les entités concernées.

Par ailleurs, les mesures envisagées sont adaptées à l'ampleur des risques qu'elles visent à atténuer. Face à ces risques, l'obligation de mettre en place des plans de sécurité et de résilience, des mécanismes de sauvegarde et des procédures de notification précoce constitue une réponse raisonnable et nécessaire pour réduire au minimum les dommages et accélérer la restauration des services.

Le règlement prévoit également des mécanismes permettant d'adapter les obligations à la situation particulière de chaque entité réglementée. Ces plans spécifiques doivent être élaborés en tenant compte des caractéristiques de chaque réseau, service ou infrastructure, afin de permettre aux opérateurs de déterminer les mesures techniques et organisationnelles les plus appropriées en fonction de leurs risques spécifiques. Cette flexibilité évite d'imposer des solutions uniformes ou rigides susceptibles d'engendrer des coûts inutiles et favorise une approche fondée sur une gestion efficace des risques.

En ce qui concerne la notification des incidents, ces obligations sont justifiées par la nécessité de disposer d'informations actualisées et fiables afin de coordonner la réponse aux incidents susceptibles d'affecter un grand nombre d'utilisateurs, d'opérateurs ou de territoires. En outre, les informations requises sont celles que les opérateurs sont déjà tenus de recueillir et de gérer en interne afin de résoudre les incidents et d'assurer la continuité de leurs services; elles n'imposent donc pas de charge administrative disproportionnée au regard des bénéfices qu'elles apportent en matière de coordination et de réactivité.

Le rapport d'évaluation de l'impact réglementaire conclut également que l'impact économique résultant de la réglementation est gérable et proportionné à l'intérêt général qu'elle vise à protéger. Bien que le coût financier estimé pour les entités réglementées soit compris entre 45 et 90 millions d'EUR, ce coût est principalement lié aux investissements visant à renforcer la résilience des infrastructures et à assurer la continuité des services essentiels. Par ailleurs, les nouvelles charges administratives sont estimées à environ 19 276 EUR, un montant faible par rapport au volume d'activité et à la taille économique des opérateurs concernés. Par ailleurs, le règlement n'entraîne aucun coût budgétaire pour les autorités publiques et n'a pas non plus d'incidence significative sur la concurrence.

Pour toutes ces raisons, on peut conclure que la mesure n'impose pas de charges excessives aux parties qui y sont soumises, mais établit plutôt des obligations proportionnées, raisonnables et nécessaires pour garantir un niveau élevé de sécurité et de résilience des réseaux et services de communications électroniques.

10. Références aux textes de base :

11. Non



EUROPEAN COMMISSION

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

12.

13. Oui

Intérêts stratégiques du pays

Les réseaux et services de communications électroniques sont des infrastructures essentielles pour la sécurité nationale, les services publics, les services d'urgence, l'activité économique et la cohésion territoriale.

14. Non

15. Oui

16.

Aspect OTC: Non

Aspects SPS: Non

Commission européenne

Point de contact Directive (UE) 2015/1535

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