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

Numéro de notification : 2023/0761/ES (Spain)

DÉCRET ROYAL APPROUVANT LE RÉGIME DE SÉCURITÉ NATIONALE POUR LES RÉSEAUX ET SERVICES 5G

Date de réception : 29/12/2023
Fin de la période de statu quo : 02/04/2024 (closed)

Message

Message 001

Communication de la Commission - TRIS/(2023) 3739

Directive (UE) 2015/1535

Notification: 2023/0761/ES

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

Notification – Notification – Notifzierung – 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 késéseket - Non fa decorrere la mora - Atidėjimai nepradedami - Atlikšanas laikposms nesākas - Ma jiftaħx 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: 20233739.FR

1. MSG 001 IND 2023 0761 ES FR 29-12-2023 ES NOTIF

2. Spain

3A. Subdirección de Asuntos Industriales, Energéticos, de Transportes, Comunicaciones y de Medioambiente
D.G. de Mercado Interior y otras Políticas Comunitarias
Ministerio de Asuntos Exteriores, UE y Cooperación

3B. Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.
Secretaría General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual.
Subdirección General de Ordenación de las Telecomunicaciones.
Ministerio de Transformación Digital

4. 2023/0761/ES - V00T - Télécommunications

5. DÉCRET ROYAL APPROUVANT LE RÉGIME DE SÉCURITÉ NATIONALE POUR LES RÉSEAUX ET SERVICES 5G

6. Réseaux et services de communications électroniques 5G

Équipements de télécommunications.

7.

8. Le règlement se compose d'une partie explicative, d'un seul article approuvant l'ENS5G (régime national de sécurité pour la 5G), de deux dispositions supplémentaires et de quatre dispositions finales.
L'ENS5G à approuver se compose de 33 articles divisés en huit chapitres et trois annexes.
L'exposé des motifs explique les raisons qui sous-tendent l'adoption du règlement et les articles du décret-loi royal en cours d'élaboration.
L'article unique approuve le régime de sécurité nationale pour les réseaux et services 5G.
La première disposition supplémentaire prévoit que le gouvernement, par décret royal, sur proposition du ministère de la transformation numérique, à la suite d'un rapport du Conseil national de sécurité, réexamine le régime de sécurité nationale pour les réseaux et services 5G lorsque les circonstances l'exigent et, en tout état de cause, tous les quatre ans.
La deuxième disposition supplémentaire prévoit que le décret-loi royal nº 7/2022 du 29 mars 2022 et l'ENS5G s'appliquent aux générations de communications électroniques antérieures à la cinquième génération, alors qu'il n'existe pas de réglementation spécifique pour celles-ci.
La première disposition finale relative au titre de compétence indique que le décret royal et le régime qu'il approuve sont délivrés en vertu des dispositions de l'article 149, paragraphe 1, point 21, et de l'article 149, paragraphe 1, point 29, de la Constitution espagnole, qui confèrent respectivement à l'État une compétence exclusive en matière de système général de télécommunications et en matière de sécurité publique.
La deuxième disposition finale dispose que la loi nº 11/2022 du 28 juin 2022 sur les télécommunications générales et ses règlements d'application serviront d'application complémentaire, et que, dans toutes les questions non réglementées par ladite législation, le décret-loi royal nº 12/2018 du 7 septembre 2018 sur la sécurité des réseaux et des systèmes d'information et la loi nº 8/2011 du 28 avril 2011 établissant des mesures de protection des infrastructures critiques, ainsi que leurs règlements d'exécution respectifs, sont d'application complémentaire.
La troisième disposition finale sur le développement réglementaire permet au chef du ministère de la transformation numérique de développer les dispositions du présent décret royal et le système qu'il approuve, et de modifier par arrêté le contenu des annexes en fonction de l'évolution du progrès technologique, l'approbation de nouvelles normes techniques et systèmes de certification pour les équipements de télécommunications et les produits connectés, et le développement de différentes configurations et paramètres techniques des réseaux et services 5G et des générations futures de communications électroniques.
La quatrième disposition finale prévoit que le règlement entre en vigueur le jour suivant celui de sa publication au «journal officiel de l'État».
En ce qui concerne le contenu de l'ENS5G, qui est approuvé:
L'article 1er dispose que le règlement est adopté en application du décret-loi royal nº 7/2022 du 29 mars 2022, notamment en application de son chapitre IV.
L'article 2 renvoie aux objectifs du règlement, qui ont déjà été analysés.
L'article 3 dispose que les définitions figurant dans le décret-loi royal nº 7/2022 du 29 mars 2022, la loi 11/2022 du 28 juin 2022 sur les télécommunications générales et le code européen des communications électroniques sont utilisées.
L'article 4 prévoit que le règlement s'applique aux opérateurs 5G, aux fournisseurs 5G et aux entreprises utilisatrices de la 5G qui ont le droit d'utiliser le domaine radioélectrique public pour installer, déployer ou exploiter un réseau privé 5G ou de fournir des services 5G à des fins professionnelles ou d'autosuffisance.
L'article 5 définit les éléments minimaux, l'infrastructure et les ressources qui constituent un réseau de communications électroniques 5G, en se référant à l'annexe I pour leur description détaillée. Il expose également les éléments critiques d'un réseau 5G, qui doit être situé, en règle générale, sur le territoire national (y compris les éventuelles exceptions).
L'article 6 fait référence au traitement global de la sécurité, conformément à la législation nationale et à celle de la communauté internationale qui a été approuvée ou qui peut l'être, obligeant les parties à effectuer, au moyen d'une méthode globale, une analyse des vulnérabilités, des menaces et des risques qui les affectent en tant qu'agents économiques et des différentes composantes, ainsi qu'une gestion adéquate et globale de ces risques par l'utilisation de techniques et de mesures appropriées pour parvenir à leur atténuation ou à leur élimination et atteindre l'objectif ultime

d'une utilisation et d'une exploitation sûres des réseaux et services 5G.
L'article 7 souligne que l'analyse et la gestion des risques constituent un élément essentiel du processus de sécurité et qu'elles devraient être une activité en cours qui est constamment mise à jour.
L'article 8 fait référence au suivi continu et à la réévaluation périodique.
L'article 9 dispose que l'analyse des risques au niveau national est celle qui figure à l'annexe II et a été effectuée en tenant compte de divers éléments tels que les informations recueillies auprès des parties assujetties, l'examen des vulnérabilités liées à la chaîne d'approvisionnement des réseaux et services 5G, l'évaluation du degré de dépendance des fournisseurs, le risque d'interruption de l'approvisionnement en raison de circonstances économiques, corporatives ou commerciales affectant les fournisseurs ou l'évaluation de l'efficacité des mesures de sécurité appliquées.
L'article 10 relatif à la gestion des risques au niveau national dispose que les critères, exigences, conditions et délais pour les parties obligées de concevoir et de mettre en œuvre des techniques et des mesures d'atténuation des risques sont ceux énoncés à l'annexe III.
L'article 11 développe les dispositions de l'article 14 du décret-loi royal nº 7/2022 du 29 mars 2022 en ce qui concerne la procédure et les aspects à évaluer par le Conseil des ministres pour la classification des fournisseurs comme étant à haut risque et les éléments à prendre en compte lors de la commande du remplacement éventuel des équipements, produits et services fournis par ces fournisseurs. De même, conformément aux dispositions du décret-loi royal susmentionné, il est précisé que les fournisseurs à haut risque dont les équipements de télécommunications, le matériel, les logiciels ou les services auxiliaires fournis sont utilisés uniquement et exclusivement sur des réseaux privés 5G ou pour la fourniture de services 5G en autosuffisance sont considérés comme des fournisseurs à risque moyen.
L'article 12 relatif à la détermination des emplacements où les équipements des fournisseurs classés comme à risque élevé ne peuvent pas être installés dispose que le Conseil national de sécurité, à la suite d'un rapport du ministère de la transformation numérique, peut déterminer les emplacements, les zones et les centres où l'équipement des fournisseurs classés comme présentant un risque élevé ne peut pas être installé. Pour l'installation, la modification ou l'adaptation de stations de radio qui assurent la couverture de ces emplacements, zones et centres, les opérateurs 5G doivent demander l'autorisation du ministère de la transformation numérique.
L'article 13 oblige les opérateurs 5G à concevoir une stratégie de diversification de la chaîne d'approvisionnement et à disposer d'équipements de transport dans le réseau d'accès mis à disposition par au moins deux fournisseurs différents. Elle prévoit également des critères qui doivent être pris en considération par le Conseil des ministres, afin de décider s'il est possible de maintenir un fournisseur unique si le nombre de fournisseurs diminue à la suite de fusions. En outre, il énonce les hypothèses et la procédure par lesquelles le ministère de la transformation numérique peut modifier la stratégie de diversification de la chaîne d'approvisionnement d'un opérateur 5G.
L'article 14 se concentre sur l'analyse des risques à effectuer par les opérateurs 5G en ce qui concerne l'ensemble des éléments, infrastructures et ressources du réseau figurant à l'annexe I, énumère les facteurs à prendre en compte et oblige les opérateurs à collecter auprès de leurs fournisseurs les pratiques et mesures de sécurité adoptées dans les produits et services qu'ils leur ont fournis et à inclure une hiérarchisation et une hiérarchie des risques en fonction de certains paramètres qui sont également énumérés. Au plus tard le 1er octobre 2024, les opérateurs 5G doivent soumettre une analyse de risque, puis tous les deux ans.
L'article 15 relatif à l'analyse des risques par les fournisseurs 5G exige l'analyse des risques liés aux équipements de télécommunications, au matériel et aux logiciels et aux services auxiliaires intervenant dans le fonctionnement ou l'exploitation des réseaux 5G ou dans la fourniture de services 5G, et la fourniture de cette analyse au ministère sur demande. Dans le cas des fournisseurs classés comme présentant un risque élevé ou moyen, l'analyse est présentée dans les six mois suivant cette classification et tous les deux ans par la suite.
L'article 16 relatif à l'analyse des risques par les entreprises utilisatrices de la 5G exige que cette analyse de risque soit fournie au ministère de la transformation numérique, lorsque ces utilisateurs sont tenus de le faire.
L'article 17 permet au ministère de la transformation numérique de recueillir auprès des parties obligées, les informations nécessaires à l'analyse des risques et classe le défaut de communication de ces informations dans un délai de 15 jours ouvrables comme une infraction grave. Les informations sont considérées comme confidentielles et ne peuvent être utilisées à d'autres fins que la réalisation des objectifs et obligations établis dans le décret-loi royal nº 7/2022 du 29 mars 2022, dans l'ENS5G et dans les actes qui sont adoptés en application des deux dispositions.
L'article 18 proclame le devoir général de toutes les parties obligées de gérer les risques de sécurité.
L'article 19 met l'accent sur la gestion de la sécurité par les opérateurs 5G, la liste des obligations pour tous les opérateurs (par exemple adopter des plans et mesures d'urgence, se conformer aux normes européennes, aux

spécifications techniques et aux systèmes de certification, faire l'objet d'un audit de sécurité à leurs propres frais ou exiger de leurs fournisseurs qu'ils se conforment aux normes de sécurité) et des obligations supplémentaires pour les opérateurs qui possèdent ou exploitent des éléments critiques d'un réseau public 5G (telles que les interdictions d'utilisation d'équipements par des fournisseurs à haut risque dans des éléments de réseau critiques ou dans certains endroits, zones et centres). Les opérateurs 5G doivent soumettre au ministère de la transformation numérique une description des mesures techniques et organisationnelles conçues et mises en œuvre pour gérer et atténuer les risques au plus tard le 1er octobre 2024 et tous les deux ans par la suite. En outre, les opérateurs 5G qui possèdent ou exploitent des éléments critiques d'un réseau public 5G doivent soumettre au ministère de la transformation numérique une stratégie de diversification de la chaîne d'approvisionnement au plus tard le 1er octobre 2024, puis chaque fois que celle-ci fait l'objet de modifications. Les informations sur l'état d'avancement de la mise en œuvre de cette stratégie doivent être communiquées au plus tard le 1er octobre de chaque année.
L'article 20 relatif à la gestion de la sécurité par les fournisseurs 5G contient une liste d'obligations, y compris la réalisation d'un audit de sécurité de leurs équipements, produits et services, la fourniture d'informations sur les interférences possibles de tiers dans la conception, la mise en service et le fonctionnement de leurs équipements, produits et services, et la collaboration avec les opérateurs 5G et les entreprises utilisatrices de la 5G en fournissant des informations et en certifiant le respect des normes et des certifications. Les fournisseurs 5G doivent préparer un rapport sur les mesures techniques et organisationnelles conçues et mises en œuvre pour gérer et atténuer les risques et fournir ledit rapport au ministère sur demande. Dans le cas des fournisseurs classés comme présentant un risque élevé ou moyen, le rapport est soumis dans les six mois suivant cette classification et tous les deux ans ensuite.
L'article 21 relatif à la gestion de la sécurité par les entreprises utilisatrices de la 5G dispose que ceux-ci ne peuvent pas utiliser dans les éléments critiques du réseau des équipements de télécommunications, des systèmes de transmission, des équipements de commutation ou d'acheminement et d'autres ressources, qui permettent le transport de signaux, de matériel, de logiciels ou de services auxiliaires par des fournisseurs classés comme présentant un risque moyen. En outre, les utilisateurs doivent fournir au ministère de la transformation numérique, sur demande, une description des mesures techniques et organisationnelles conçues et mises en œuvre pour gérer et atténuer les risques.
L'article 22 relatif à la gestion de la sécurité par les administrations publiques dispose que, pour des raisons de sécurité nationale, lors de l'installation, du déploiement et de l'exploitation des réseaux 5G, qu'ils soient publics ou privés, ou de la fourniture de services 5G, qu'ils soient accessibles au public ou à des fins d'autosuffisance, les administrations publiques ne peuvent pas utiliser d'équipements, de produits et de services fournis par des fournisseurs à haut risque ou à risque moyen.
L'article 23 dispose que, dans le respect des obligations prévues aux articles précédents, les parties obligées tiennent compte et appliquent ce qui est établi dans le décret-loi royal nº 7/2022 du 29 mars 2022, dans l'ENS5G et dans les actes qui sont adoptés en application des deux dispositions.
L'article 24 permet au ministère de la transformation numérique de recueillir auprès des parties obligées les informations nécessaires à la gestion des risques et classe le défaut de communication de ces informations dans un délai de 15 jours ouvrables comme une infraction grave. Les informations sont considérées comme confidentielles et ne peuvent être utilisées à d'autres fins que la réalisation des objectifs et obligations établis dans le décret-loi royal nº 7/2022 du 29 mars 2022, dans l'ENS5G et dans les actes qui sont adoptés en application des deux dispositions.
L'article 25 dispose que toutes les parties obligées, ainsi que les administrations publiques, les fabricants, les importateurs, les distributeurs et ceux qui mettent sur le marché et vendent des équipements et dispositifs terminaux pour se connecter à un réseau 5G et être en mesure de fournir des services 5G doivent coopérer et soumettre les informations nécessaires à la modification et à la mise en œuvre de l'ENS5G.
L'article 26 dispose que, par arrêté du chef du ministère de la transformation numérique, l'utilisation d'un équipement, d'un système, d'un programme ou d'un service spécifique peut faire l'objet d'une certification préalable en vertu du règlement (UE) 2019/881 du Parlement européen et du conseil du 17 avril 2019 relatif à la cybersécurité, ou au titre de systèmes de certification et de normes techniques pour la certification des équipements et produits 5G susceptibles d'être approuvés au niveau européen ou international.
L'article 27 dispose que le règlement s'applique sans préjudice du droit des investissements étrangers et du droit de la concurrence.
L'article 28 relatif aux équipements terminaux prévoit que la fabrication, l'importation, la distribution, la mise sur le marché et la vente d'équipements et de dispositifs terminaux destinés à être connectés à un réseau 5G et à la fourniture des services 5G sont subordonnés au respect des exigences de sécurité applicables aux produits numériques et des

exigences essentielles applicables en matière de cybersécurité, adoptées conformément à la législation européenne, notamment en ce qui concerne la protection des données à caractère personnel, la protection de la vie privée et la protection contre la fraude.
L'article 29 fait référence à la coopération internationale que doit développer le ministère de la transformation numérique, en particulier au niveau de l'Union européenne.
L'article 30 fait référence à la compétence du ministère de la transformation numérique pour la mise en œuvre de l'ENS5G. Le ministère devrait coordonner ses activités avec les autres organismes chargés de la cybersécurité et des infrastructures critiques afin d'assurer une mise en œuvre cohérente de l'ENS5G.
L'article 31 définit les pouvoirs de mise en œuvre de l'ENS5G qui correspondent au ministère de la transformation numérique, y compris, par exemple, l'élaboration, la spécification et le détail du contenu de l'ENS5G, la réalisation d'audits visant à vérifier et à contrôler le respect des obligations imposées et l'octroi d'aides publiques.
L'article 32 attribue au ministère de la transformation numérique tous les pouvoirs de la fonction d'inspection.
L'article 33 sur le régime des sanctions renvoie aux dispositions des articles 30 et 31 du décret-loi royal nº 7/2022 du 29 mars 2022.
L'annexe I décrit les éléments, l'infrastructure et les ressources qui constituent un réseau 5G.
L'annexe II contient l'analyse des risques au niveau national.
L'annexe III définit la gestion des risques au niveau national.

9. Les communications mobiles de cinquième génération ou 5G constituent un nouveau paradigme des communications électroniques avec un grand potentiel de transformation au bénéfice de la société et de l'économie, car elles rendent possible l'intégration de nouvelles fonctionnalités qui auront un grand impact comme l'informatique en réseau et permettent la création de réseaux virtuels, offrant une faible latence et fournissant des services à haute valeur ajoutée dans des domaines tels que la médecine, les transports et l'énergie.
Par conséquent, l'Union européenne et l'Espagne encouragent le déploiement rapide des réseaux 5G et la mise en œuvre de projets démontrant leur utilité pour différents secteurs grâce à la fourniture de services 5G.
Les réseaux et services 5G présentent des avantages comparatifs en matière de sécurité par rapport aux générations précédentes. Cependant, ils présentent également des risques spécifiques découlant, par exemple, de leur architecture de réseau plus complexe, ouverte et désagrégée, et de leur capacité à transporter d'énormes volumes d'informations et à permettre l'interaction simultanée de personnes et de choses multiples. Leur interconnexion avec d'autres réseaux et le caractère transnational d'un grand nombre de menaces ont un impact sur leur sécurité, et l'utilisation généralisée prévisible de ces réseaux pour des fonctions économiques et sociétales essentielles augmentera l'impact potentiel des incidents de sécurité dont ils souffrent.
Ces nouveaux risques spécifiques pour la sécurité des communications mobiles 5G ont été traités en termes réglementaires par le décret-loi royal nº 7/2022 du 29 mars 2022 relatif aux exigences visant à garantir la sécurité des réseaux et services de communications électroniques de cinquième génération, qui intègre pleinement la recommandation (UE) 2019/534 de la Commission européenne du 26 mars 2019 sur la cybersécurité des réseaux 5G, ainsi que les recommandations que la communication de la Commission européenne du 29 janvier 2020 sur le déploiement sécurisé de la 5G dans l'Union — Mise en œuvre de la boîte à outils de l'Union (COM/2020/50 final) a fourni aux États membres en ce qui concerne l'utilisation de cette boîte à outils.
Le décret-loi royal nº 7/2022 du 29 mars 2022, précité, prévoit son développement réglementaire par le biais du système de sécurité nationale pour les réseaux et services 5G (ENS5G).
Conformément à l'article 5, paragraphe 3, du décret-loi royal susmentionné, l'ENS5G procède à un traitement complet de la sécurité des réseaux et services 5G, en tenant compte des contributions à la portée de chaque agent de la chaîne de valeur 5G, ainsi que des règlements, recommandations et normes techniques de l'Union européenne, de l'Union internationale des télécommunications (UIT) et d'autres organisations internationales, afin de garantir l'objectif ultime d'une utilisation et d'une exploitation sécurisées des réseaux et services 5G en Espagne.
De son côté, l'article 20 du décret-loi royal prévoit que, afin d'assurer le fonctionnement continu et sécurisé du réseau et des services 5G, l'ENS5G procède à une analyse des risques au niveau national sur la sécurité des réseaux et services 5G et identifie, précise et développe des mesures d'atténuation et de gestion des risques analysés.
Enfin, conformément à l'article 21 du décret-loi royal, l'ENS5G est approuvé par le gouvernement, par décret royal, sur proposition du ministère de la transformation numérique, à la suite d'un rapport du Conseil national de sécurité.
Le présent règlement approuve l'ENS5G, développant les dispositions du décret-loi royal nº 7/2022 du 29 mars 2022

relatif aux exigences visant à garantir la sécurité des réseaux et services de communications électroniques de cinquième génération.

10. Références aux textes de base:

11. Non

12.

13. Non

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