MINISTÈRE DE LA TRANSFORMATION NUMÉRIQUE

SECRÉTARIAT D'ÉTAT AUX TÉLÉCOMMUNICATIONS ET AUX INFRASTRUCTURES NUMÉRIQUES

SECRÉTARIAT GÉNÉRAL DES TÉLÉCOMMUNICATIONS ET DE L'ORGANISATION DES SERVICES DE MÉDIAS AUDIOVISUELS

RAPPORT D'ANALYSE D'IMPACT RÉGLEMENTAIRE DU PROJET DE DÉCRET ROYAL APPROUVANT LE RÉGIME DE SÉCURITÉ NATIONALE POUR LES RÉSEAUX ET SERVICES 5G.

RÉSUMÉ ANALYTIQUE

Ministère et/ou organisme à l'origine de la proposition	Ministère de la transformation numérique Secrétariat d'État aux télécommunications et aux infrastructures numériques	Date	Décembre 2023
Titre de la réglementation	PROJET DE DÉCRET ROYAL APPROUVANT LE SYSTÈME DE SÉCURITÉ NATIONALE POUR LES RÉSEAUX ET SERVICES 5G		
Type de rapport	Normal ☒ Abrégé ☐		
CHAMP D'APPLICATION DE LA PROPOSITION			
Domaines réglementés	En application des dispositions du décret-loi royal 7/2022 du 29 mars 2022 relatif aux exigences visant à garantir la sécurité des réseaux et services de communications électroniques de cinquième génération, en particulier, en application du chapitre IV, la proposition approuve le système de sécurité nationale pour les réseaux et services 5G [Esquema Nacional de Seguridad de las redes y servicios 5G] (ci-après l'«ENS5G»), afin de créer un environnement fiable pour le développement et l'adoption de réseaux et de services 5G.		
Objectifs	- Effectuer un traitement complet et intégral 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; - assurer le fonctionnement continu et sécurisé du réseau et		

	des services 5G; - piloter la sécurité de bout en bout de l'écosystème généré par la technologie 5G; - renforcer la sécurité dans l'installation et l'exploitation des réseaux de communications électroniques 5G et dans la fourniture de services de communications mobiles et sans fil soutenus par les réseaux 5G; - promouvoir un marché suffisamment diversifié pour les fournisseurs des réseaux et services de communications électroniques 5G, afin d'assurer la sécurité sur la base de raisons techniques, stratégiques et opérationnelles et d'éviter, pour ces raisons, la présence de fournisseurs présentant une cote de risque élevé ou moyenne dans certains éléments ou zones de réseau; - renforcer la protection de la sécurité nationale; - renforcer l'industrie et promouvoir les activités nationales de R&D&I en matière de cybersécurité liées à la technologie 5G.
Principales solutions envisagées	Il n'y a pas d'alternative à l'approbation de ce règlement, puisque l'article 21 du décret-loi royal 7/2022 du 29 mars 2022 oblige le gouvernement à approuver, par décret royal, sur proposition du ministère de la transformation numérique, à la suite d'un rapport du Conseil national de sécurité, un système de sécurité nationale pour les réseaux et services 5G.
CONTENU, ANALYSE JURIDIQUE ET DESCRIPTION DU PROCESSUS	
Type de règlement	Décret royal
Structure du règlement	Le projet se compose d'une partie explicative, d'un seul article approuvant l'ENS5G, 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.
Rapports à recueillir	- Rapport CNMC; - procédure d'information dans le domaine des

	réglementations techniques et des règles relatives aux services de la société de l'information prévue par la directive (UE) 2015/1535; - rapport du Secrétariat général technique du ministère de la transformation numérique; - rapport du secrétariat technique général du ministère de la transition écologique et du défi démographique; - rapport du Conseil national de sécurité; - avis du Conseil d'État.	
Procédure d'audition	Conformément aux dispositions de l'article 26, paragraphe 2, de la loi 50/1997, du 27 novembre 1997, du gouvernement et de l'article 133, paragraphe 1, de la loi 39/2015, du 1er octobre 2015, de la procédure administrative commune des administrations publiques, entre le 30 mai et le 22 juin 2022, une consultation publique préalable a été menée, sur le site internet du ministère de l'économie et de la transformation numérique. De même, la procédure d'audience publique est menée, conformément aux dispositions des articles 26, paragraphe 6, de la loi 50/1997, du 27 novembre 1997, et 133, paragraphe 2, de la loi 39/2015, du 1er octobre 2015.	
ANALYSE D'IMPACT		
Respect de la répartition des pouvoirs	Le décret royal et le régime qu'il approuve relèvent des compétences de l'État dans le domaine des télécommunications et de la sécurité publique, établies aux articles 149, paragraphe 1, point 21), et 149, paragraphe 1, point 29) de la Constitution.	
Impact économique et budgétaire	Impact économique global	Selon des études de la Commission européenne, les bénéfices estimés de l'introduction de la 5G dans quatre secteurs de production (automobile, santé, transports et services publics) augmenteraient progressivement à 62,5 milliards d'euros par an dans l'Union européenne, ce qui s'élèverait à 113 milliards d'euros en ajoutant les incidences

		indirectes. La même étude estime que l'Espagne bénéficierait d'avantages indirects de 14,6 milliards d'euros dans les quatre secteurs examinés ainsi que d'une forte croissance de l'emploi. La confiance dans la sécurité des réseaux et services 5G est essentielle pour étendre leur utilisation entre les citoyens et les entreprises.
	En ce qui concerne la concurrence	☐ Le règlement n'a pas d'effets significatifs sur la concurrence. ☒ Le règlement a des effets positifs sur la concurrence. ☒ Le règlement a des effets négatifs sur la concurrence.
	Du point de vue des charges administratives	☐ Il implique une réduction des charges administratives. ☐ Il intègre de nouvelles charges administratives. ☒ Cela n'affecte pas la charge administrative.
	Du point de vue budgétaire, le	

	règlement: ☒ N'affecte pas les budgets des administrations publiques ☒ N'affecte pas les budgets de l'administration de l'État	☐ Entraîne une dépense ☐ Entraîne des recettes
Impact sur l'égalité des sexes	Le règlement a une incidence sur le genre de la manière suivante	Négatif ☐ Aucun ☒ Positif ☐
Autres impacts envisagés		-Impact sur la lutte contre le dépeuplement et le changement climatique. -Impact sur l'égalité des chances, la non-discrimination et l'accessibilité universelle pour les personnes handicapées. -Impact sur les enfants, les adolescents et la famille.
Autres points		

A. CHAMP D'APPLICATION DE LA PROPOSITION

1. MOTIVATION

- **Causes:**

Les communications mobiles de cinquième génération ou 5G constituent un nouveau paradigme des communications électroniques avec un potentiel de transformation majeure au bénéfice de la société et de l'économie, car elles ouvrent la possibilité d'intégrer de nouvelles fonctionnalités qui auront une incidence majeure, comme l'informatique en réseau, et permettent de créer des réseaux virtuels, d'offrir une faible latence et de fournir des services à forte valeur ajoutée dans des domaines tels que la médecine, les transports et l'énergie.

L'Union européenne et l'Espagne encouragent donc le déploiement rapide des réseaux 5G et la réalisation 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 d'objets multiples. Leur interconnexion avec d'autres réseaux et le caractère transnational de nombreuses menaces ont une incidence sur leur sécurité, et l'utilisation généralisée prévisible de ces réseaux pour des fonctions essentielles à l'économie et à la société augmentera l'incidence potentielle des incidents de sécurité qu'ils pourraient subir.

Ces nouveaux risques spécifiques pour la sécurité des communications mobiles 5G ont été traités par le décret-loi royal 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 relative à la cybersécurité des réseaux 5G, ainsi que les recommandations que la communication de la Commission européenne du 29 janvier 2020 sur le déploiement sûr de la 5G dans l'Union «Mise en œuvre de la boîte à outils de la Commission européenne» (COM/2020/50 final) a fournies aux États membres en ce qui concerne l'utilisation de cette «boîte à outils».

Le décret-loi royal 7/2022 du 29 mars 2022, précité, prévoit son développement réglementaire par l'intermédiaire du système national de sécurité des réseaux et des services 5G (ENS5G).

Conformément à l'article 5, paragraphe 3, du décret-loi royal susmentionné, l'ENS5G procédera 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 de l'utilisation et de l'exploitation sûres 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 effectuera une analyse des risques au niveau national sur la sécurité des réseaux et services 5G et identifiera, précisera et développera des mesures d'atténuation et de gestion des risques analysés.

Enfin, conformément à l'article 21 du décret-loi royal, l'ENS5G sera 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.

Ce règlement approuve l'ENS5G, développant les dispositions du décret-loi royal 7/2022 du 29 mars 2022 relatif aux exigences visant à garantir la sécurité des réseaux et services de communications électroniques de cinquième génération.

- **Groupes concernés:**

Le règlement s'appliquera:

a) Aux personnes physiques ou morales exploitant des réseaux 5G et aux fournisseurs de services de communications électroniques basés en tout ou en partie sur ces réseaux 5G.

   Il s'agit notamment des opérateurs mobiles qui détiennent des concessions administratives pour l'utilisation du spectre radioélectrique et des opérateurs mobiles virtuels, ainsi qu'aux opérateurs utilisant la technologie 5G pour fournir des services de communication. Il comprend également des opérateurs exploitant des réseaux de communications électroniques privés (ou corporatifs), qui seront plus fréquents avec la 5G qu'avec la technologie 4G.

b) aux fournisseurs d'équipements et de services pour l'exploitation des réseaux et services 5G, externes aux opérateurs (collectivement désignés dans le règlement comme «fournisseurs»).

Une partie du règlement les affecte directement, c'est-à-dire qu'elle contient des dispositions susceptibles d'être appliquées et sanctionnées par les autorités compétentes. Il concerne, d'une part, les obligations de collaboration dans les fonctions de surveillance de l'administration et, d'autre part, les exigences de certification des produits, procédés ou services, ou de soumission à l'audit que le règlement impose.

Toutefois, le règlement les affecte également indirectement, en exigeant des opérateurs de réseaux et de services 5G qu'ils respectent les exigences de sécurité vis-à-vis de leurs fournisseurs. Cet ensemble de règles comprend des dispositions qui peuvent avoir une incidence significative sur les fournisseurs. Par exemple: la loi prévoit que les opérateurs peuvent être tenus de cesser totalement ou partiellement leurs relations avec certains fournisseurs classés comme présentant un risque élevé;

c) Utilisateurs corporatifs des réseaux 5G.

Il peut s'agir d'entités qui gèrent une couche ou un segment du réseau pour leurs propres besoins (p. ex., un hôpital pour ses applications de médecine à distance). En raison de leur interface avec le réseau principal, ils peuvent être une passerelle vers une attaque extérieure.

En outre, dans la mesure où il assure la sécurité des réseaux et services 5G, le règlement profite à tous les utilisateurs de ces réseaux et services, en particulier les administrations publiques, qui peuvent les utiliser comme un canal sûr et efficace de communication avec les citoyens.

- **Questions d'intérêt public**

L'intérêt public concerné est d'assurer une protection maximale des réseaux et services de communication fondés sur la technologie 5G et les réseaux contre les attaques ou les incidents de sécurité, afin de renforcer la confiance dans les nouveaux services 5G.

L'utilisation généralisée prévisible de ces réseaux dans des fonctions essentielles à l'économie et à la société, et la dépendance vis-à-vis des fournisseurs externes, signifie qu'en période de fortes tensions géopolitiques, la cybersécurité des réseaux 5G devient une priorité de sécurité nationale.

En outre, il existe des droits fondamentaux, tels que le droit à la vie privée et familiale ou au secret des communications, garanti au plus haut niveau réglementaire par la Constitution espagnole.

À long terme, le renforcement de l'autonomie technologique de l'Union européenne est également impliqué.

En outre, étant donné le potentiel de cette technologie pour la croissance de différents secteurs économiques, la croissance économique et sociale de l'Espagne et le bien-être des citoyens qui accèdent aux services essentiels ou exercent leur droit à l'information par le biais des réseaux 5G sont également affectés.

- **Pourquoi c'est le moment approprié pour le faire:**

Les opérateurs devraient adapter dès que possible leurs politiques de cybersécurité aux mesures énoncées dans le règlement, afin que les réseaux et services de communications mobiles de cinquième génération soient sécurisés dès le départ.

En outre, il convient de rappeler que le deuxième paragraphe de la troisième disposition finale du décret-loi royal 7/2022, du 29 mars 2022, a fixé un délai de six mois à compter de son entrée en vigueur pour l'approbation de l'ENS5G, qui a déjà été dépassé.

2. Objectifs.

L'objectif du règlement est d'assurer la fiabilité des réseaux et services 5G, et donc le développement de services à valeur ajoutée pour l'économie et la société, dans des domaines aussi divers que les transports, les soins de santé, l'industrie, l'agriculture, la logistique, l'énergie ou les médias.

À cette fin, des objectifs spécifiques sont fixés:

- effectuer un traitement complet et intégral 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;
- assurer le fonctionnement continu et sécurisé du réseau et des services 5G;
- piloter la sécurité de bout en bout de l'écosystème généré par la technologie 5G;
- renforcer la sécurité dans l'installation et l'exploitation des réseaux de communications électroniques 5G et dans la fourniture de services de communications mobiles et sans fil soutenus par les réseaux 5G;
- promouvoir un marché suffisamment diversifié pour les fournisseurs des réseaux et services de communications électroniques 5G, afin d'assurer la sécurité sur la base de raisons techniques, stratégiques et opérationnelles et d'éviter, pour ces raisons, la présence de fournisseurs présentant une cote de risque élevé ou moyenne dans certains éléments ou zones de réseau;
- renforcer la protection de la sécurité nationale;

- renforcer l'industrie et promouvoir les activités nationales de R&D&I en matière de cybersécurité liées à la technologie 5G.

3. Alternatives

Il n'y a pas d'alternative à l'approbation de ce règlement, puisque l'article 21 du décret-loi royal 7/2022 du 29 mars 2022 oblige le gouvernement à approuver, par arrêté royal, sur proposition du ministère de la transformation numérique, à la suite d'un rapport du Conseil national de sécurité, un système national de sécurité des réseaux et services 5G.

4. Respect des principes d'une saine réglementation.

La loi est conforme aux principes de bonne réglementation énoncés à l'article 129 de la loi 39/2015 du 1er octobre 2015 relative à la procédure administrative commune des administrations publiques.

Le principe de nécessité est respecté, puisque ce décret royal est émis par le décret-loi royal 7/2022 du 29 mars 2022, afin de garantir un objectif d'intérêt général, tel que la sécurité et la confiance dans les communications électroniques.

Il respecte le principe de proportionnalité, étant donné que les mesures sont adaptées aux risques recensés dans chaque cas.

Le règlement respecte le principe de sécurité juridique dès qu'il met en œuvre les dispositions du décret-loi royal 7/2022 du 29 mars 2022 relatif aux exigences visant à garantir la sécurité des réseaux et services de communications électroniques de cinquième génération, et complète le cadre réglementaire actuel en matière de sécurité, en ajoutant des exigences et des contrôles uniquement lorsque l'unicité des réseaux et services 5G et de leurs risques l'exige.

Le principe de transparence est respecté, car les parties prenantes ont pu participer à la procédure d'élaboration du règlement et seront publiées.

Enfin, le principe d'efficacité est respecté, étant donné que les charges administratives ont été limitées au minimum nécessaire pour atteindre l'objectif d'assurer la sécurité des réseaux et des services 5G.

5. Plan législatif annuel

Le décret-loi royal 7/2022 du 29 mars 2022 correspond au projet de loi sur les exigences visant à assurer la sécurité des réseaux et services de communications électroniques de cinquième génération, prévu dans le plan législatif annuel de l'administration générale de l'État pour 2022, approuvé par accord du Conseil des ministres du 11 janvier 2022.

Ce projet, qui met en œuvre ce décret-loi royal, n'est toutefois pas prévu dans le plan législatif annuel 2023.

B. CONTENU, ANALYSE JURIDIQUE ET DESCRIPTION DE LA PROCÉDURE

1. Contenu.

Le règlement se compose d'une partie explicative, d'un seul article approuvant l'ENS5G, 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.

La partie explicative explique les raisons de l'adoption du règlement et les articles du décret-loi royal qui sont mis en œuvre.

L'article unique approuve le système de sécurité nationale des réseaux et services 5G.

La première disposition additionnelle prévoit que le gouvernement, par arrêté royal, sur proposition du ministère de la transformation numérique, à la suite d'un rapport du Conseil national de sécurité, réexaminera le système national de sécurité des réseaux et services 5G lorsque les circonstances l'entraîneront et, en tout état de cause, tous les quatre ans.

La deuxième disposition supplémentaire prévoit que le décret-loi royal 7/2022 du 29 mars 2022 et l'ENS5G s'appliqueront aux générations de communications électroniques après la cinquième génération, tant qu'il n'y a pas de réglementation spécifique à leur égard.

La première disposition finale relative au titre de compétence indique que l'arrêté royal et le régime qu'il approuve sont délivrés en vertu des dispositions des articles 149, paragraphe 1, point 21) et 149, paragraphe 1, point 29) de la Constitution, qui confèrent à l'État une compétence exclusive en matière de régime général des télécommunications et en matière de sécurité publique, respectivement.

La deuxième disposition finale déclare que la loi générale 11/2022, du 28 juin 2022, sur les télécommunications et ses règlements d'application, est d'application supplémentaire, et dispose que, dans toutes les matières non réglementées par ladite législation, le décret-loi royal 12/2018, du 7 septembre 2018, sur la sécurité des réseaux et des systèmes d'information

et la loi 8/2011, du 28 avril 2011, établissant des mesures de protection des infrastructures critiques, ainsi que ses règlements de développement respectifs, seront d'application supplémentaire.

La troisième disposition finale sur le développement réglementaire permet au titulaire du ministère de la transformation numérique de mettre en œuvre les dispositions du présent arrêté royal et du système qu'il approuve, et de modifier par ordre le contenu des annexes en fonction de l'évolution du progrès technologique, l'approbation de nouvelles normes techniques et systèmes de certification des équipements de télécommunication et des 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 entrera 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 7/2022 du 29 mars 2022, notamment en application du chapitre IV de celui-ci;

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 7/2022 du 29 mars 2022, la loi générale 11/2022 du 28 juin 2022 sur les télécommunications et le code européen des communications électroniques seront utilisées;

l'article 4 prévoit que le règlement s'appliquera aux opérateurs 5G, aux fournisseurs de 5G et aux entreprises utilisatrices de la 5G qui ont des droits d'utilisation dans le domaine radioélectrique public pour installer, déployer ou exploiter un réseau privé 5G ou pour fournir des services 5G à des fins professionnelles ou autonomes;

l'article 5 identifie les éléments, infrastructures et ressources minimales qui constituent un réseau de communications électroniques 5G, en renvoyant sa description détaillée à l'annexe I. Il définit également les éléments critiques d'un réseau 5G, qui est situé, en tant que règlement général, sur le territoire national (recueil d'éventuelles exceptions);

l'article 6 fait référence au traitement global de la sécurité conformément à la législation communautaire et nationale internationale approuvée ou susceptible d'être approuvée, qui impose aux parties obligées d'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 pour atteindre l'objectif ultime de l'exploitation et de l'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 des activités courantes et constamment mises 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 figurant à l'annexe II et qu'elle a été réalisée en tenant compte de divers éléments tels que les informations recueillies auprès des parties obligées, 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, liées à l'entreprise 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 met en œuvre les dispositions de l'article 14 du décret-loi royal 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, ainsi que 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 télécommunication, le matériel, les logiciels ou les services auxiliaires fournis sont uniquement et exclusivement utilisés dans les réseaux privés 5G, ou pour la fourniture de services 5G en autonomie, sont considérés comme des fournisseurs à risque moyen;

l'article 12, relatif à la détermination des emplacements où des équipements de fournisseurs qualifiés à haut risque 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 dans lesquels l'équipement des fournisseurs qualifiés à haut risque 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 demandent l'autorisation au 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 dans le réseau d'accès, des équipements de transport

fournis par au moins deux fournisseurs différents. Il prévoit également des critères à prendre en compte par le Conseil des ministres, afin de décider s'il est possible de maintenir un fournisseur unique si le nombre de fournisseurs est réduit en raison des concentrations d'entreprises. Il met également en évidence les hypothèses et la procédure par lesquelles le ministère de la transformation numérique est en mesure de modifier la stratégie de diversification dans la chaîne d'approvisionnement d'un opérateur 5G;

l'article 14 est axé sur l'analyse des risques à effectuer par les opérateurs de la 5G en ce qui concerne l'ensemble des éléments, infrastructures et ressources du réseau énumérés à l'annexe I; les facteurs à prendre en compte sont énumérés, les opérateurs sont tenus de rechercher auprès de leurs fournisseurs les pratiques et mesures de sécurité adoptées dans les produits et services qu'ils leur ont fournis et d'inclure une priorisation et une hiérarchie des risques en fonction de certains paramètres qui sont également énumérés. Au plus tard le 1er octobre 2024, les opérateurs 5G soumettent une analyse de risque, puis tous les deux ans par la suite;

l'article 15, relatif à l'analyse des risques par les fournisseurs 5G, exige l'analyse des risques liés aux équipements, matériels et logiciels de télécommunications et aux services auxiliaires liés au fonctionnement ou à l'exploitation des réseaux 5G ou à la fourniture de services 5G, et la communication de cette analyse au ministère si nécessaire. Dans le cas de fournisseurs classés comme à risque élevé ou à risque moyen, l'analyse est soumise dans les six mois suivant cette estimation et tous les deux ans par la suite;

l'article 16, relatif à l'analyse des risques par les entreprises utilisatrices de la 5G, oblige à fournir cette analyse de risque 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 qualifie d'infraction grave le défaut de communication de ces informations dans un délai de 15 jours ouvrables. 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 7/2022, du 29 mars 2022, dans l'ENS5G, et dans les actes qui sont émis en exécution 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 (telles que l'adoption de plans et de mesures d'urgence, le respect des normes, spécifications et systèmes de certification européens, l'exécution, à leurs frais, d'un audit de sécurité ou l'obligation pour leurs fournisseurs de se conformer aux normes de sécurité) et d'autres pour les opérateurs qui possèdent ou exploitent des éléments critiques

d'un réseau public 5G (telles que l'interdiction d'utiliser des équipements par des fournisseurs à haut risque dans des éléments de réseau critiques ou dans certains endroits, zones et centres). Les opérateurs 5G soumettent au ministère de la transformation numérique une description des mesures techniques et organisationnelles conçues et mises en œuvre pour gérer et atténuer les risques avant 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 soumettent au ministère de la transformation numérique une stratégie de diversification de la chaîne d'approvisionnement avant le 1er octobre 2024 et par la suite chaque fois qu'elle fait l'objet de modifications. Les informations sur l'état d'avancement de la mise en œuvre de cette stratégie sont 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 qui comprennent 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, le fonctionnement et le fonctionnement de leurs équipements, produits et services; ou 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 prépareront un rapport sur les mesures techniques et organisationnelles conçues et mises en œuvre pour gérer et atténuer les risques et fournir un tel rapport au ministère si nécessaire. Dans le cas des fournisseurs classés comme présentant un risque élevé ou moyen, le rapport est soumis dans les six mois suivant cette estimation, puis tous les deux ans;

l'article 21, relatif à la gestion de la sécurité par les entreprises utilisatrices de la 5G, dispose qu'elles ne peuvent pas utiliser dans les éléments critiques du réseau des systèmes de transmission d'équipements de télécommunication, des équipements de commutation ou d'acheminement et d'autres ressources permettant le transport de signaux, de matériel, de logiciels ou de services auxiliaires de fournisseurs qui ont été classés comme présentant un risque moyen, et qu'ils doivent fournir au ministère de la transformation numérique, le cas échéant, une description des mesures techniques et organisationnelles conçues et appliquées pour gérer et atténuer les risques;

l'article 22, relatif à la gestion de la sécurité par les administrations publiques.(AP), dispose que, pour des raisons de sécurité nationale, lors de l'installation, du déploiement et de l'exploitation de réseaux 5G, publics ou privés, ou de la fourniture de services 5G, accessibles au public ou autonomes, les AP 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, conformément aux obligations prévues aux articles précédents, les parties obligées tiennent compte et appliquent les dispositions du décret-loi royal 7/2022, du

29 mars 2022, de 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 assujetties les informations nécessaires à la gestion des risques et qualifie d'infraction grave le défaut de communication de ces informations dans un délai de 15 jours ouvrables. 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 7/2022, du 29 mars 2022, dans l'ENS5G, et dans les actes qui sont émis en exécution 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 commercialisent des équipements et dispositifs terminaux pour se connecter à un réseau 5G et être en mesure de fournir des services 5G, coopèrent et envoient les informations nécessaires à la modification et à l'exécution de l'ENS5G;

l'article 26 dispose que, par ordre de la personne responsable au 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 des systèmes de certification et des normes techniques pour la certification des équipements et produits 5G qui peuvent être approuvés au niveau européen ou international;

l'article 27 dispose que le règlement s'applique sans préjudice des règles relatives aux investissements étrangers et à la concurrence;

l'article 28, relatif aux équipements terminaux, prévoit que la fabrication, l'importation, la distribution, la mise sur le marché et la mise sur le marché d'équipements et de dispositifs terminaux pour se connecter à un réseau 5G et être en mesure de fournir des services 5G seront subordonnés au respect des exigences de sécurité des 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 vie privée et la protection contre la fraude;

l'article 29 concerne la coopération internationale à développer par 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 et pour la coordination avec les autres organismes responsables de la cybersécurité et des infrastructures critiques afin d'assurer une mise en œuvre cohérente de l'ENS5G;

l'article 31 définit les pouvoirs pour la mise en œuvre de l'ENS5G qui incombent au ministère de la transformation numérique, parmi lesquels figurent, par exemple, le développement, 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 ou 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, relatif au régime des sanctions, renvoie aux dispositions des articles 30 et 31 du décret-loi royal 7/2022 du 29 mars 2022;

l'annexe I décrit les éléments, infrastructures et 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.

2. Analyse juridique

- **Relations avec d'autres réglementations nationales**.

- Le règlement met en œuvre le décret-loi royal 7/2022, du 29 mars 2022, relatif aux exigences visant à garantir la sécurité des réseaux et services de communications électroniques de cinquième génération, et notamment son chapitre IV, relatif à l'ESN5G;

- la loi 9/2014 du 9 mai 2014 (en particulier son article 44) contient des obligations de sécurité génériques que les opérateurs de réseau 5G respectent toujours;

- le décret-loi royal 12/2018 du 7 septembre 2018 relatif à la sécurité des réseaux et des systèmes d'information établit les exigences auxquelles les opérateurs désignés comme opérateurs critiques en vertu de la loi 8/2011 du 28 avril 2011 établissant des mesures de protection des infrastructures critiques continuent de se conformer;

- l'ordonnance IET/1090/2014, du 16 juin 2014, réglementant les conditions relatives à la qualité du service dans la fourniture de services de communications électroniques réglemente, au chapitre VI, la notification obligatoire aux autorités des cas d'interruption du service téléphonique et de l'accès à Internet et son chapitre VII, se réfère au pouvoir d'inspecteur du Secrétariat d'État aux télécommunications et aux infrastructures numériques;

- le plan national de cybersécurité approuvé le 29 mars 2022 par le Conseil des ministres précise, au moyen d'actions et de projets spécifiques, différentes mesures incluses dans la stratégie nationale de cybersécurité de 2019;

- le règlement est également compatible avec le volet 15 du plan espagnol pour la reprise, la transformation et la résilience, qui vise à assurer la connectivité sur l'ensemble du territoire national, à diriger le déploiement de réseaux et de services basés sur les technologies 5G en Europe et à positionner l'Espagne comme un pôle international d'infrastructures et de talents en matière de cybersécurité. Cette composante est formulée à travers deux plans fondamentaux de la stratégie numérique du gouvernement espagnol (España Digital 2025): le plan pour la connectivité et les infrastructures numériques; et la stratégie de renforcement technologique de la 5G.

- **Cohérence avec le droit de l'Union européenne:**

- Le code des communications électroniques européen, établi par la directive 2018/1972 du 11 décembre 2018, exige que des mesures soient prises pour garantir la sécurité des réseaux et des services et pour prévenir ou réduire au minimum l'incidence des incidents de sécurité;

- le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) et la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), sont également liés à ce règlement, étant donné que le renforcement de la sécurité des réseaux 5G entraînera une protection accrue contre les ingérences illégitimes dans le droit à la vie privée et le secret des communications dans ce domaine;

- le règlement est également conforme à la directive sur la sécurité des réseaux et de l'information (SRI), adoptée en 2016, qui établit des obligations de sécurité pour les opérateurs de services essentiels (dans des secteurs vitaux tels que l'énergie, les transports, la santé et la finance) et les fournisseurs de services numériques (marchés en ligne, moteurs de recherche et services en nuage) et avec sa révision de 2022 (directive SRI2);

- ce projet met en œuvre la recommandation (UE) 2019/534 de la Commission du 26 mars 2019, Cybersécurité des réseaux 5G, qui proposait une action coordonnée par les États membres pour analyser les risques pour la sécurité de la technologie 5G ainsi que la collecte et la mise en œuvre de bonnes pratiques pour assurer la sécurité de ces réseaux. Les États membres ont soutenu cette recommandation dans les conclusions adoptées par le Conseil de l'Union européenne le 3 décembre 2019;

- À la suite de la recommandation visée au paragraphe précédent, la boîte à outils européenne a été publiée le 29 janvier 2020. Le même jour, la Commission européenne a publié la communication intitulée «Déploiement sécurisé de la 5G dans l'Union – Mise en œuvre de la boîte à outils de l'Union», qui indique que les conclusions et les actions recommandées dans la boîte à outils sont des «mesures clés» à mettre en œuvre par les États membres et la Commission européenne pour assurer la sécurité de ces réseaux en Europe;

- le règlement est également conforme au règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à la cybersécurité, qui régit la procédure d'adaptation des systèmes européens de certification de cybersécurité des technologies de l'information et de la communication;

- enfin, le règlement porte sur la proposition de règlement sur la cyberrésilience, qui vise à établir des exigences de cybersécurité obligatoires pour les produits constitués d'équipements informatiques (matériel) et de logiciels comportant des éléments numériques connectés.

- **Règlements qui sont modifiés ou abrogés**

Aucun règlement n'est modifié ou abrogé.

- **Entrée en vigueur**

Conformément à sa quatrième disposition finale, l'arrêté royal entrera en vigueur le jour suivant celui de sa publication au «Journal officiel de l'État».

Conformément aux dispositions de l'article 23 de la loi 50/1997 du 27 novembre 1997 du gouvernement, cela est justifié par la nécessité d'établir dans les meilleurs délais les règles applicables aux déploiements 5G déjà effectués par les opérateurs, en évitant d'éventuels incidents de sécurité.

En outre, il convient de rappeler que le deuxième alinéa de la troisième disposition finale du décret-loi royal 7/2022 du 29 mars 2022 a établi un délai de six mois à compter de son entrée en vigueur, pour l'approbation de l'ENS5G, qui a déjà été dépassé.

3. Description du processus

- **Participation du public**

Conformément aux dispositions de l'article 26, paragraphe 2, de la loi 50/1997, du 27 novembre 1997, du gouvernement et de l'article 133, paragraphe 1, de la loi 39/2015, du 1er octobre 2015, concernant la procédure administrative commune des administrations publiques, afin de faire connaître l'opinion des opérateurs, des citoyens et de toute partie intéressée sur l'élaboration d'un nouveau règlement sur le système national de sécurité des réseaux 5G entre le 30 mai et le 22 juin 2022, une consultation publique préalable a été menée, par l'intermédiaire du bureau électronique du ministère de l'économie et de la transformation numérique.

Au cours de la consultation susmentionnée, 15 contributions ont été reçues, qui ont été prises en compte lors de l'élaboration de la proposition de règlement.

En particulier, 14 contributions ont été reçues d'entités et 1 d'une personne:

- AMETIC (20/06/22);
- ASSOCIATION ESPAGNOLE DE NORMALISATION, UNE (20/06/22);
- CHAMBRE DE COMMERCE D'ESPAGNE (20/06/22);
- CEOE (20/06/22);
- DIGITALES (20/06/22);
- ERICSSON (20/06/22);
- HUAWEI TECHNOLOGIES ESPAÑA, S.L. (20/06/22);
- MASMOVIL IBERCOM, S.A.U. (20/06/22);
- NOKIA ESPAÑA (20/06/22);
- ORANGE ESPAGNE, S.A.U. (20/06/22) (CONFIDENTIEL);
- SAMSUNG ELECTRONICS IBERIA, S.A.U. (19/06/22);
- TELEFÓNICA ESPAÑA (20/06/22) (CONFIDENTIEL);
- VODAFONE ESPAÑA, S.A.U. ET VODAFONE ONO, S.A.U. (20/06/22);
- ZTE ESPAÑA, S.L.U. (20/06/22);
- MIGUEL BAÑÓN (16/06/22).

De même, la procédure d'audience publique est menée, conformément aux dispositions des articles 26, paragraphe 6, de la loi 50/1997, du 27 novembre 1997, et 133, paragraphe 2, de la loi 39/2015, du 1er octobre 2015.

- **Rapports à recueillir**

-

- Rapport CNMC;

- procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information prévue par la directive (UE) 2015/1535;

- rapport du Secrétariat général technique du ministère de la transformation numérique;

- rapport du Secrétariat général technique du ministère de la transition écologique et du défi démographique;

- rapport du Conseil national de sécurité;

- avis du Conseil d'État.

C. RESPECT DE LA RÉPARTITION DES POUVOIRS

Le règlement est conforme à l'ordre constitutionnel de répartition des compétences, délivré en vertu des compétences exclusives en matière de télécommunications et de sécurité publique conférées à l'État par les articles 149, paragraphe 1, point 21) et 149, paragraphe 1, point 29) de la Constitution espagnole (CE).

En ce qui concerne les compétences exclusives de l'État dans le domaine des télécommunications et le système général de communication à **l'article 149, paragraphe 1, point 21),** de la CE, la première d'entre elles est liée aux aspects techniques des émissions liées à l'utilisation d'ondes radioélectriques ou électromagnétiques (domaine radioélectrique public), ce qui justifie une «régulation conjointe de toutes les variantes de télécommunications et de communications radioélectriques» (STC 78/2017, du 22 juin, FJ 4 a), citant STC 168/1993 du 27 mai, FJ 4). Pour sa part, la compétence exclusive de l'État en ce qui concerne le «régime général des communications» «comprend, bien entendu, l'ensemble des pouvoirs réglementaires qui lui sont conférés (SSTC 84/1982, FJ 4, et 38/1983, FJ 3); mais cela implique également un plus», puisqu'il «peut impliquer l'attribution des compétences d'exécution nécessaires à la mise en place d'un système matériellement unitaire (STC 195/1996, 28 novembre, FJ 6)». Dès lors, il relève de la compétence de l'article 149, paragraphe 1, point 21), de la CE de réglementer les services de communications électroniques fournis par

toute technologie et donc également de garantir la disponibilité et la «sécurité» des réseaux ou des services, terme défini dans le code des communications électroniques européen, comme «la capacité des réseaux et services de communications électroniques à résister, avec un certain degré de confiance, à toute action compromettant la disponibilité, l'authenticité, l'intégrité et la confidentialité de ces réseaux et services, des données stockées, traitées ou transmises, ainsi que la sécurité des services connexes que ces réseaux et services de communications électroniques offrent ou rendent accessibles».

Comme STC 8/2016 du 21 janvier 2016, FJ 3, rappelle: «D'un point de vue plus global, cela intègre également dans le domaine des télécommunications et des systèmes généraux de communications (et donc l'État a une compétence exclusive en vertu de l'article 149, paragraphe 1, point 21), de la CE) la formation, la réglementation ou la configuration du secteur des télécommunications lui-même (communications électroniques) en tenant compte de la convergence technologique (et des services) et du cadre réglementaire des communications électroniques de l'Union européenne afin d'assurer une réglementation homogène dans toute l'Espagne. Cette homogénéité est nécessaire, non seulement pour le développement et l'innovation du secteur, mais aussi pour la garantie des droits des citoyens dans le cadre de la société de l'information (ou société de la connaissance), étant donné que le développement des communications et des nouvelles technologies de l'information est un facteur essentiel pour parvenir à la cohésion sociale, économique et territoriale nécessaire pour éviter, ou du moins réduire, la fracture dite numérique».

En ce qui concerne le titre de compétence en matière de sécurité publique à **l'article 149, paragraphe 1, point 23),** nous nous référons aux dispositions du FTJ de l'arrêt 142/2018 du 20 décembre 2018, qui viennent d'être transcrites, ainsi qu'aux paragraphes précédents en ce qui concerne l'utilisation généralisée prévisible de ces réseaux dans des fonctions essentielles pour l'économie et la société, compte tenu du fait que la dépendance à l'égard de fournisseurs externes exige qu'à un moment tel que celui actuel de graves tensions géopolitiques, la cybersécurité des réseaux 5G devienne un objectif prioritaire de sécurité nationale, au sein duquel la sécurité publique est encadrée.

C'est ce qui ressort de l'arrêt de la Cour constitutionnelle 84/2016 du 3 novembre 2016, selon lequel «on peut dire qu'il existe une coïncidence substantielle entre le sens et la finalité des titres de compétence dans les points 4) et 29) de l'article 149, paragraphe 1 de la CE et la notion de sécurité nationale, définie à l'article 3 de la loi 36/2015, comme suit: «l'action de l'État vise à protéger la liberté, les droits et le bien-être des citoyens, à garantir la défense de l'Espagne et de ses principes et valeurs constitutionnels, ainsi qu'à contribuer, avec nos partenaires et alliés, à la sécurité internationale dans le respect des engagements pris».

Enfin, il convient de noter que les communautés autonomes et les entités locales ont eu l'occasion de se prononcer sur le projet de règlement dans le cadre de la procédure de consultation publique menée entre le 30 mai et le 20 juin 2022 sans qu'aucune d'entre elles ne soumette de contributions. Elles peuvent également participer à la procédure d'audition publique correspondante.

D. IMPACT ÉCONOMIQUE ET BUDGÉTAIRE.

1. Impact économique global.

Les communications électroniques ont été un secteur très dynamique et innovant, généralement lié à des investissements dans le déploiement de nouveaux réseaux.

À l'heure actuelle, il est possible de poursuivre cette dynamique innovante, grâce à des investissements dans les réseaux 5G, mais cela ne sera possible que si des mesures appropriées sont prises pour assurer l'intégrité, la continuité et la sécurité de ces réseaux, en évitant les risques que leur déploiement généralisé pourrait entraîner.

En outre, en raison de sa nature transversale, le secteur des télécommunications non seulement assure la fourniture de services de plus en plus essentiels, tels que le télétravail, la télémédecine et l'apprentissage en ligne, mais il favorise également la croissance d'autres secteurs, tels que l'industrie du contenu, les méga données, l'Internet des objets et les services de voitures connectées. Cela permet une gestion intelligente des transports et des ressources énergétiques et contribue à combler le fossé numérique entre les différentes régions.

En ce sens, les nouveaux réseaux 5G sont positionnés comme un élément clé pour accélérer la transformation numérique de la société et de l'économie.

Dans notre environnement plus immédiat, les analyses de la Commission européenne prévoient que l'impact économique annuel direct des avantages escomptés de l'introduction de la 5G dans quatre secteurs productifs (automobile, santé, transports et services publics) au sein de l'UE augmenterait progressivement à 62,5 milliards d'euros d'ici 2025, et à 113 milliards d'euros compte tenu de l'impact indirect. Selon la même étude, l'Espagne bénéficierait d'avantages indirects de 14,6 milliards d'euros dans les quatre secteurs examinés ainsi que d'une forte croissance de l'emploi.

En conclusion, il convient de noter qu'en ces temps d'incertitude internationale, les télécommunications sont l'un des secteurs les plus dynamiques de l'économie et, en raison de leur caractère transversal, figurent parmi les plus susceptibles de contribuer à la croissance, à

la productivité et à l'emploi, et donc aussi au développement économique et au bien-être social.

Les mesures de sécurité proposées dans le projet préliminaire devraient également avoir une incidence neutre sur les prix, étant donné que les opérateurs et les fournisseurs de services font déjà des investissements importants pour assurer la connectivité par l'intermédiaire de la 5G, la sécurité étant un aspect marginal de ces coûts.

En tout état de cause, l'effort économique consacré aux mesures de sécurité est considéré comme un investissement, dans la mesure où il réduit le coût de remplacement du service et d'éventuelles compensations, tout en augmentant les recettes provenant de l'entrée de nouveaux clients qui dépendent de la nouvelle technologie.

En raison de son incidence intersectorielle, l'introduction de la technologie 5G devrait créer un effet positif important sur l'emploi dans de nombreux secteurs.

Bien qu'en outre, le respect des mesures de sécurité spécifiques prévues par le présent règlement aura également un effet positif sur la création d'emplois dans des secteurs tels que la R&D&I, la certification ou l'audit, l'objectif spécifique du règlement étant de renforcer l'industrie et de promouvoir la R&D&I au niveau national dans le domaine de la cybersécurité.

L'effet de la loi sur les consommateurs devrait également être positif, étant donné que le choix accru entre les technologies résultant de l'introduction de la 5G ajoute lui-même les avantages intangibles associés à une plus grande sécurité et confiance dans l'utilisation de la nouvelle technologie.

2. Effets sur la concurrence et l'unité du marché

Le règlement a des effets positifs, car les dispositions relatives à la diversification des fournisseurs dans la chaîne d'approvisionnement et les mesures visant à renforcer l'industrie et à promouvoir la R&D&I au niveau national dans le domaine de la cybersécurité peuvent contribuer à l'émergence et à la croissance de nouveaux acteurs.

D'autre part, les restrictions à la libre concurrence résultant de la restriction de la participation des fournisseurs à haut risque ou à risque moyen préservent la sécurité nationale en assurant la continuité des services et applications essentiels qui s'appuient sur ces réseaux (santé, protection civile, éducation, etc.) et ne sont essentielles qu'à la lumière d'une analyse rigoureuse des risques et des décisions prises par d'autres États membres ou par l'Union elle-même.

Par conséquent, étant donné que le règlement devrait avoir des effets à la fois positifs et négatifs sur la concurrence, les deux devraient se contrecarrer, créant ainsi une nouvelle

situation concurrentielle dans laquelle de nouveaux fournisseurs contribuent à l'autonomie technologique de l'Union européenne, évitant ainsi les risques découlant des cyberattaques.

3. Incidence budgétaire

- **Du point de vue des recettes:**

Le projet n'implique pas la production ou la prévision de recettes pour le Trésor public ou pour la Trésorerie d'autres administrations publiques.

- **Du point de vue des dépenses:**

Le projet n'impliquera pas la réalisation de dépenses provenant des budgets généraux de l'État, ni la prise en charge de coûts ou de dépenses pour le Trésor public ou pour le Trésor d'autres administrations publiques.

Les tâches de coordination, d'inspection et de sanction confiées au ministère de la transformation numérique seront exécutées avec les moyens et les ressources déjà affectés à ce ministère.

E. DÉTECTION ET MESURE DES CHARGES ADMINISTRATIVES.

Aucune nouvelle charge n'est imposée, étant donné que les charges administratives pesant sur les opérateurs, les fournisseurs et les entreprises utilisatrices étaient déjà prévues par le décret-loi royal 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 est en cours de développement, de sorte que nous devons nous référer à la mesure des charges contenue dans le MAIN de ce règlement.

F. INCIDENCE SUR L'ÉGALITÉ DES SEXES

Le projet n'a aucune incidence sur le genre, car son contenu ne contient aucune mesure susceptible d'affecter l'égalité des chances entre les femmes et les hommes.

G. IMPACT SUR LA LUTTE CONTRE LE DÉPEUPLEMENT ET LE CHANGEMENT CLIMATIQUE

La sécurité de la technologie 5G est un élément clé de la structuration territoriale du pays, étant donné que l'accès sécurisé aux nouveaux réseaux et aux nouveaux contenus et services numériques qui peuvent être fournis par leur intermédiaire est un élément essentiel pour

l'intégration des citoyens et des entreprises dans la société de l'information et de la connaissance, favorisant ainsi la cohésion sociale et le développement économique et contribuant au développement de la nouvelle administration en ligne.

En ce sens, les mesures introduites par la loi deviennent des piliers importants pour parvenir à l'élimination de la fracture numérique et pour structurer différents territoires afin que l'accès à de nouveaux services et applications tels que la télémédecine, l'apprentissage en ligne ou le télétravail puisse être garanti n'importe où en Espagne, favorisant ainsi l'implantation et la fixation de la population dans les zones rurales.

En outre, les télécommunications sont un facteur clé de la lutte contre le changement climatique. Cela inclut l'objectif de l'Union européenne de réduire les émissions de gaz à effet de serre de 55 % par rapport aux niveaux de 1990 d'ici 2030.

Le secteur des technologies de l'information et de la communication génère relativement peu d'émissions, tout en pouvant jouer un rôle essentiel dans la lutte contre le changement climatique en facilitant une utilisation plus efficace des ressources énergétiques dans d'autres secteurs.

En ce sens, il convient de souligner les économies d'énergie des réseaux eux-mêmes, grâce à l'amélioration de l'efficacité énergétique des technologies 5G, ainsi qu'au rôle transformateur que le secteur des TIC dans son ensemble a joué dans l'innovation et la refonte des modèles économiques de tous les secteurs à l'ère dite numérique, ce qui en fait le catalyseur dont les autres secteurs ont besoin pour contribuer à la nouvelle économie à faibles émissions de gaz à effet de serre, en facilitant les utilisations innovantes de produits et de services «intelligents», contribuant à générer des avantages environnementaux et permettant des économies d'énergie pour les utilisateurs.

En outre, les télécommunications sont très utiles pour la surveillance de l'environnement et du climat, y compris les prévisions météorologiques, et essentielles pour les communications en matière d'alerte rapide et d'atténuation des effets des catastrophes.

Les conclusions de l'étude «Télécommunications et CO2: Le rôle de la technologie mobile contre le changement climatique» indique que 13 initiatives technologiques mobiles peuvent réduire les émissions de CO2 de 113 millions de tonnes (équivalent aux émissions d'environ 50 millions de véhicules) et générer des économies d'énergie de 43 milliards d'euros en Europe.

Cela nécessitera 1,04 milliard de nouvelles connexions mobiles, dont 87 % seraient de machine à machine (M2M).

Son application en Espagne entraînerait une réduction de 10,6 millions de tonnes d'émissions de CO2 (équivalent aux émissions générées par 4,7 millions de véhicules, soit 15 %

du parc actuel), et des économies d'énergie de 4,042 milliards d'euros. Dans le cas de l'Espagne, cela nécessitera 98 millions de nouvelles connexions, dont 85 millions de M2M.

Les économies d'énergie proviendront principalement d'une utilisation accrue des services intelligents M2M (réseaux électriques intelligents, logistique intelligente, villes intelligentes et systèmes de production intelligents) ainsi que du remplacement des activités physiques par des activités virtuelles.

Ce processus de virtualisation remplacerait les processus, les mouvements, les réunions et les déplacements par des solutions virtuelles à faibles émissions. Voici quelques exemples: réduire les déplacements en utilisant des salles de réunion virtuelles dotées d'une connectivité de télécommunication, promouvoir l'utilisation de produits de télécommunications afin que les employés puissent travailler à distance à partir de chez eux, et utiliser les communications mobiles pour améliorer les processus de commerce électronique et faciliter les systèmes de commande et d'expédition pour les achats. Ces initiatives nous permettraient non seulement de nous adapter à d'éventuelles mesures de confinement sanitaire en cas d'épidémies, mais aussi de réduire les émissions de CO2 en Europe de plus de 22 millions de tonnes, ainsi que les économies potentielles de consommation d'énergie de 14,1 milliards d'euros (en Espagne: réduction de 2 millions de tonnes d'émissions de CO2 et de 1,33 milliard d'euros).

H. AUTRES INCIDENCES

Le projet de loi n'a aucune incidence sur l'égalité des chances, la non-discrimination ou l'accessibilité universelle des personnes handicapées.

Il n'y a pas non plus d'incidence significative du projet de loi sur l'enfance, l'adolescence ou la famille.