RECOMMANDATIONS

RECOMMANDATION (UE) 2019/534 DE LA COMMISSION

du 26 mars 2019

Cybersécurité des réseaux 5G

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 292,

considérant ce qui suit:

(1) Pour la Commission, le déploiement de la 5e génération (5G) de technologies de réseau constitue un catalyseur majeur des futurs services numériques et une priorité dans le cadre de la stratégie pour un marché unique numérique. La Commission a adopté le plan d'action pour la 5G de manière que l'Union dispose de l'infrastructure de connectivité nécessaire à sa transformation numérique à partir de 2020 ([1]).

(2) Les réseaux 5G s'appuieront sur l'actuelle 4e génération (4G) de technologies de réseau pour fournir de nouvelles capacités de service et devenir l'infrastructure centrale et le catalyseur de pans considérables de l'économie de l'Union. Une fois déployés, les réseaux 5G constitueront la cheville ouvrière d'un large éventail de services essentiels au fonctionnement du marché intérieur et au maintien et à l'exercice de fonctions sociétales et économiques vitales, dans les domaines de l'énergie, des transports, de la banque et de la santé, ainsi que des systèmes de commande industriels, par exemple. L'organisation de processus démocratiques tels que les élections s'appuiera aussi de plus en plus sur l'infrastructure numérique et les réseaux 5G.

(3) Le fait que de nombreux services critiques dépendent des réseaux 5G rendrait particulièrement graves les conséquences de perturbations systémiques et étendues. Dès lors, la cybersécurité des réseaux 5G est une question d'importance stratégique pour l'Union, à l'heure où les cyberattaques se multiplient et sont plus sophistiquées que jamais.

(4) Vu le caractère interconnecté et transnational des infrastructures qui sous-tendent l'écosystème numérique et la nature transfrontière des menaces, toute vulnérabilité importante et/ou tout incident de cybersécurité majeur concernant les réseaux 5G dans un État membre auraient des répercussions sur l'Union dans son ensemble. C'est pourquoi des mesures devraient être prises pour soutenir un niveau élevé commun de cybersécurité des réseaux 5G.

(5) La nécessité d'agir au niveau de l'Union a été confirmée par les États membres. Dans ses conclusions du 21 mars 2019, le Conseil européen a déclaré attendre avec intérêt une recommandation de la Commission relative à une approche concertée en matière de sécurité des réseaux 5G ([2]).

(6) Garantir la souveraineté européenne devrait être un objectif majeur, dans le plein respect des valeurs d'ouverture et de tolérance de l'Europe ([3]). Laisser dans des mains étrangères les investissements dans des secteurs stratégiques, l'acquisition d'actifs, de technologies et d'infrastructures critiques dans l'Union et la fourniture d'équipements critiques peut également présenter des risques pour la sécurité de l'Union.

(7) La cybersécurité des réseaux 5G est essentielle pour garantir l'autonomie stratégique de l'Union, comme indiqué dans la communication conjointe intitulée «Les relations UE-Chine — Une vision stratégique» ([4]).

(8) Dans sa résolution sur les menaces pour la sécurité liées à la présence technologique croissante de la Chine dans l'Union, le Parlement européen invite également la Commission et les États membres à prendre des mesures au niveau de l'Union ([5]).

(9) La présente recommandation porte sur les risques liés à la cybersécurité des réseaux 5G et définit des orientations relatives à l'adoption de mesures appropriées d'analyse et de gestion des risques au niveau national, à la mise en place d'une évaluation coordonnée des risques au niveau européen et au lancement d'un processus d'élaboration d'une «boîte à outils» commune comprenant les meilleures mesures de gestion des risques.

(10) Un cadre législatif solide est en place au niveau de l'Union pour protéger les réseaux de communications électroniques.

([1]) COM(2016) 588 final.
([2]) Conclusions du Conseil européen des 21 et 22 mars 2019.
([3]) État de l'Union 2018 — L'heure de la souveraineté européenne, 12 septembre 2018.
([4]) JOIN(2019) 5 final.
([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//FR

(11) Le cadre de l'Union dans le domaine des communications électroniques ([6]) favorise la concurrence, soutient le marché intérieur, défend les intérêts des utilisateurs finals et, avec le code des communications électroniques européen ([7]), poursuit un objectif de connectivité supplémentaire, articulé autour de résultats: l'accès étendu de l'ensemble des citoyens et des entreprises de l'Union à la connectivité fixe et mobile à très haute capacité et l'adoption à grande échelle de ladite connectivité, associés à la préservation des intérêts des citoyens. La directive 2002/21/CE impose aux États membres de garantir l'intégrité et la sécurité des réseaux de communications publics, en veillant à ce que les entreprises fournissant des réseaux de communications publics ou des services de communications électroniques accessibles au public prennent des mesures techniques et organisationnelles pour gérer le risque en matière de sécurité des réseaux et des services de manière appropriée. Elle dispose également que les autorités réglementaires nationales compétentes ont des pouvoirs, dont celui de donner des instructions contraignantes, pour assurer le respect de ces obligations.

(12) En outre, la directive 2002/20/CE du Parlement européen et du Conseil ([8]) autorise les États membres à assortir une autorisation générale de conditions relatives à la sécurité des réseaux publics face aux accès non autorisés, afin de protéger la confidentialité des communications conformément à la directive 2002/58/CE du Parlement européen et du Conseil ([9]).

(13) Pour favoriser le respect de ces obligations, l'Union a mis en place un certain nombre d'organes de coopération. L'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), la Commission, les États membres et les autorités réglementaires nationales ont élaboré des orientations techniques à l'intention des autorités réglementaires nationales concernant la notification des incidents, les mesures de sécurité, ainsi que les menaces et les actifs ([10]). Le groupe de coopération institué par la directive (UE) 2016/1148 du Parlement européen et du Conseil ([11]) (ci-après le «groupe de coopération») réunit les autorités compétentes afin de soutenir et de faciliter la coopération, notamment en fournissant des orientations stratégiques pour les activités du réseau des centres de réponse aux incidents de sécurité informatique, qui facilite la coopération opérationnelle au niveau technique.

(14) Le futur cadre européen de certification en matière de cybersécurité ([12]) devrait constituer un instrument d'appui essentiel pour promouvoir des niveaux de sécurité cohérents. Il devrait permettre la mise en place de systèmes de certification de cybersécurité pour répondre aux besoins des utilisateurs d'équipements et de logiciels liés à la 5G. Compte tenu de l'importance cruciale de ces infrastructures, l'élaboration de systèmes européens de certification de cybersécurité des produits, services ou processus des technologies de l'information et de la communication utilisés pour les réseaux 5G devrait constituer une priorité immédiate. Les États membres et les acteurs du marché devraient participer activement à la mise au point de ces systèmes de certification, en apportant notamment leur appui à la définition de profils de protection spécifiques pour les réseaux 5G.

(15) En l'absence d'harmonisation législative au niveau de l'Union, les États membres peuvent préciser, au moyen de règlements techniques nationaux adoptés conformément au droit de l'Union, qu'un système européen de certification de cybersécurité devrait être obligatoire. Les États membres ont également recours aux systèmes européens de certification de cybersécurité dans le cadre des marchés publics et de la directive 2014/24/UE du Parlement européen et du Conseil ([13]) et pourraient soutenir la mise au point de mécanismes d'aide — tels qu'une plateforme d'assistance — pour l'acquisition de solutions de cybersécurité par les acheteurs publics.

(16) Un niveau élevé de protection des données et de la vie privée est un élément important aux fins de la sécurité des réseaux 5G. Des règles ont également été définies au niveau de l'Union pour garantir la sécurité du traitement des données à caractère personnel, y compris dans le cadre de communications électroniques. Le règlement général sur la protection des données ([14]) établit l'obligation de traiter les données à caractère personnel de façon à en garantir la sécurité, y compris pour prévenir tout accès non autorisé aux données et aux installations de traitement ainsi que toute utilisation non autorisée desdites données et installations. La directive «vie privée et communications électroniques» établit des règles spécifiques relatives à la protection de la confidentialité des

([6]) Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive «cadre») (JO L 108 du 24.4.2002, p. 33) et directives particulières.

([7]) Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (JO L 321 du 17.12.2018, p. 36).

([8]) Directive 2002/20/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'autorisation de réseaux et de services de communications électroniques (directive «autorisation») (JO L 108 du 24.4.2002, p. 21).

([9]) 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) (JO L 201 du 31.7.2002, p. 37).

([10]) https://resilience.enisa.europa.eu/article-13

([11]) Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

([12]) Proposition de règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) no 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité) [COM(2017) 477 final — 2017/0225(COD)].

([13]) Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65).

([14]) 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) (JO L 119 du 4.5.2016, p. 1).

communications et de l'équipement terminal de l'utilisateur final. Elle impose également aux fournisseurs de services de prendre les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de leurs services.

(17) L'Union a également adopté un instrument destiné à protéger les infrastructures et les technologies critiques, telles que celles utilisées dans le cadre des communications, en permettant aux États membres de filtrer les investissements directs étrangers pour des motifs de sécurité ou d'ordre public et en créant un dispositif de coopération permettant aux États membres et à la Commission d'échanger des informations et de soulever des préoccupations concernant des investissements spécifiques ([15]).

(18) Les États membres et les opérateurs prennent actuellement d'importantes mesures préparatoires pour permettre le déploiement à grande échelle des réseaux 5G. Plusieurs États membres ont exprimé des préoccupations concernant les risques potentiels pour la sécurité liés aux réseaux 5G dans le cadre de la mise en œuvre des procédures d'octroi de droits d'utilisation dans les bandes de fréquences destinées aux réseaux 5G ([16]) et étudient les mesures à prendre pour faire face à ces risques.

(19) Lorsque l'on aborde les risques pour la cybersécurité liés aux réseaux 5G, il convient de tenir compte à la fois de facteurs techniques et d'autres facteurs. Les facteurs techniques peuvent inclure les vulnérabilités de cybersécurité susceptibles d'être exploitées pour obtenir un accès non autorisé à des informations (cyberespionnage, pour des raisons économiques ou politiques) ou à d'autres fins malveillantes (cyberattaques visant à perturber ou à détruire des systèmes et des données). Des aspects importants à prendre en considération devraient être la nécessité de protéger les réseaux tout au long de leur cycle de vie et celle de couvrir tous les équipements pertinents, y compris durant les phases de conception, de développement, de passation de marchés, de déploiement, d'exploitation et de maintenance des réseaux 5G.

(20) Les autres facteurs peuvent comprendre les exigences réglementaires ou autres imposées aux fournisseurs d'équipements des technologies de l'information et de la communication. Une évaluation de l'importance de ces facteurs devrait tenir compte, entre autres, du risque global d'influence d'un pays tiers, compte tenu notamment de son modèle de gouvernance, de l'absence d'accords de coopération en matière de sécurité ou d'arrangements similaires, tels que des décisions d'adéquation, relatifs à la protection des données entre l'Union et le pays tiers concerné ou de la participation de ce pays à des accords multilatéraux, internationaux ou bilatéraux ayant trait à la cybersécurité, à la lutte contre la cybercriminalité ou à la protection des données.

(21) Une évaluation des risques devrait être menée à bien au niveau national en tant qu'étape importante de l'élaboration d'une approche européenne de la cybersécurité des réseaux 5G. Elle aiderait les États membres à adapter en conséquence leurs mesures nationales relatives aux exigences de sécurité et à la gestion des risques.

(22) Il y a lieu de développer la coordination afin de garantir l'efficacité des mesures visant à faire face à ces menaces pour la cybersécurité, mesures qui sont essentielles au bon fonctionnement du marché intérieur et à la protection des données à caractère personnel et de la vie privée.

(23) Les évaluations nationales des risques devraient servir de base à une évaluation coordonnée des risques au niveau de l'Union, constituée d'un inventaire des menaces et d'un examen conjoint réalisé par les États membres avec le soutien de la Commission et en association avec l'Agence de l'Union européenne pour la cybersécurité (ENISA).

(24) À la lumière des évaluations des risques réalisées au niveau national et à celui de l'Union, le groupe de coopération devrait élaborer une «boîte à outils» recensant les types de risques pour la cybersécurité et les types de mesures pouvant être prises pour atténuer les risques dans des domaines tels que la certification, les essais et les contrôles d'accès. Il devrait également définir les mesures spécifiques qui pourraient être appropriées pour faire face aux risques recensés par un ou plusieurs États membres. Le groupe de coopération devrait s'appuyer sur l'Agence de l'Union européenne pour la cybersécurité (ENISA), Europol, l'Organe des régulateurs européens des communications électroniques (ORECE) et le Centre de situation et du renseignement de l'Union européenne. Cette «boîte à outils» devrait servir à conseiller la Commission sur la mise au point d'exigences minimales communes contribuant à garantir un niveau élevé de cybersécurité des réseaux 5G dans l'ensemble de l'Union.

(25) Dans le cadre des mesures prises pour faire face aux risques pour la cybersécurité, il convient d'envisager de promouvoir la cybersécurité par la diversité des fournisseurs lors de la constitution de tout réseau unique.

([15]) Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union (JO L 79 I du 21.3.2019, p. 1).

([16]) La procédure d'enchères relative à au moins une bande de fréquences est prévue pour 2019 dans 11 États membres: l'Allemagne, l'Autriche, la Belgique, la France, la Grèce, la Hongrie, l'Irlande, la Lituanie, les Pays-Bas, le Portugal et la Tchéquie. Six autres procédures d'enchères sont prévues pour 2020: en Espagne, en Lituanie (fréquences différentes), à Malte, en Pologne, au Royaume-Uni et en Slovaquie. *Source:* http://5gobservatory.eu/observatory-overview/observatory-reports/

(26) La présente recommandation devrait être sans préjudice des compétences des États membres en ce qui concerne les activités relatives à la sécurité publique, à la défense et à la sécurité nationale et les activités de l'État dans le domaine du droit pénal, y compris le droit des États membres d'exclure des fournisseurs de leur marché pour des raisons de sécurité nationale,

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

I. **OBJECTIFS**

1. Pour soutenir l'élaboration d'une approche de l'Union visant à garantir la cybersécurité des réseaux 5G, la présente recommandation recense les mesures qui devraient être prises afin de permettre que:

   a) les États membres évaluent les risques en matière de cybersécurité concernant les réseaux 5G au niveau national et prennent les mesures de sécurité nécessaires;

   b) les États membres et les institutions, agences et autres organes de l'Union concernés effectuent conjointement une évaluation coordonnée des risques au niveau de l'Union, en s'appuyant sur les évaluations nationales des risques;

   c) le groupe de coopération institué par la directive (UE) 2016/1148 (le «groupe de coopération») établisse un train de mesures communes qui pourraient être prises pour atténuer les risques en matière de cybersécurité liés aux infrastructures qui sous-tendent l'écosystème numérique, en particulier les réseaux 5G.

II. **DÉFINITIONS**

2. Aux fins de la présente recommandation, on entend par:

   a) «réseau 5G»: un ensemble composé de tous les éléments des infrastructures de réseau pertinents pour la technologie de communication sans fil et mobile utilisés pour la connectivité et des services à valeur ajoutée et offrant des performances avancées telles que des capacités et des vitesses de débit très élevées, des communications à temps de latence faibles, une excellente fiabilité, ou supportant un nombre élevé d'appareils connectés. Ils peuvent inclure des éléments provenant de réseaux préexistants utilisant les générations précédentes de technologie de communication sans fil et mobile, comme la 4G ou la 3G. Les réseaux 5G devraient être réputés inclure tous les éléments pertinents du réseau;

   b) «infrastructures qui sous-tendent l'écosystème numérique»: les infrastructures utilisées aux fins de la numérisation dans toute une série d'applications critiques pour l'économie et la société.

III. **MESURES PRISES AU NIVEAU NATIONAL**

3. Les États membres devraient réaliser, d'ici au 30 juin 2019, une évaluation des risques liés aux infrastructures des réseaux 5G, afin notamment de recenser les éléments les plus sensibles, sur lesquels des atteintes à la sécurité auraient des conséquences négatives importantes. Pour la même date, les États membres devraient également examiner les exigences en matière de sécurité et les méthodes de gestion des risques applicables au niveau national pour prendre en considération les menaces pesant sur la cybersécurité susceptibles de découler i) de facteurs techniques, comme les caractéristiques techniques propres aux réseaux 5G et ii) d'autres facteurs, comme le cadre juridique et politique auquel les fournisseurs d'équipement des technologies de l'information et de la communication peuvent être soumis dans les pays tiers.

4. En se fondant sur cette analyse de risques et cet examen au niveau national et en tenant compte de l'action coordonnée actuellement menée au niveau de l'Union, les États membres devraient:

   a) actualiser les exigences en matière de sécurité et les méthodes de gestion des risques afférentes aux réseaux 5G;

   b) actualiser les obligations pertinentes imposées aux entreprises fournissant des réseaux de communications publics ou des services de communications électroniques accessibles au public conformément aux articles 13 *bis* et 13 *ter* de la directive 2002/21/CE;

   c) assortir l'autorisation générale de conditions relatives à la sécurité des réseaux publics face aux accès non autorisés et demander aux entreprises qui participeront aux prochaines procédures de sélection pour l'octroi de l'utilisation des radiofréquences des bandes 5G de s'engager à respecter les exigences de sécurité des réseaux conformément à la directive 2002/20/CE;

   d) appliquer d'autres mesures préventives destinées à atténuer les risques potentiels en matière de cybersécurité.

5. Parmi les mesures visées au point 4 devraient figurer l'obligation renforcée, pour les fournisseurs et les opérateurs, de garantir la sécurité de parties sensibles des réseaux, ainsi que l'obligation de fournir, s'il y a lieu, des informations pertinentes aux autorités nationales compétentes concernant les changements qu'il est prévu d'apporter aux réseaux de communications électroniques et des exigences concernant le test préalable, par des laboratoires de certification/d'audit nationaux, de la sécurité et de l'intégrité de certains composants et systèmes informatiques.

6. Des contrôles conjoints de la sécurité devraient être effectués par deux États membres, ou plus, en utilisant et en partageant l'expertise et les moyens techniques appropriés liés aux infrastructures qui sous-tendent l'écosystème numérique et les réseaux 5G, par exemple lorsqu'une même entreprise exploite ou met en place une infrastructure de réseau dans plusieurs États membres ou lorsque des configurations de réseaux présentent de nombreuses similitudes. L'Agence de l'Union européenne pour la cybersécurité (ENISA), Europol et l'Organe des régulateurs européens des communications électroniques (ORECE) devraient accorder la priorité aux demandes d'aide dans ce domaine émanant d'États membres. Les résultats de ces contrôles devraient être transmis au groupe de coopération et au réseau des centres de réponse aux incidents de sécurité informatique.

IV. ACTION COORDONNÉE AU NIVEAU DE L'UNION

7. Les États membres devraient entamer des activités, d'ici au 30 avril 2019, dans le cadre d'un axe de travail spécifique au sein du groupe de coopération afin d'élaborer une approche commune visant à faire face aux risques pour la cybersécurité en lien avec les réseaux 5G. Les États membres devraient inviter les autorités compétentes à participer, s'il y a lieu, aux travaux du groupe de coopération.

Évaluation coordonnée des risques au niveau européen

8. Les États membres devraient échanger des informations entre eux ainsi qu'avec les organismes compétents de l'Union pour favoriser une prise de conscience commune des risques existants et potentiels en matière de cybersécurité associés aux réseaux 5G.

9. Les États membres devraient transmettre leurs évaluations nationales des risques à la Commission et à l'Agence de l'Union européenne pour la cybersécurité (ENISA) au plus tard le 15 juillet 2019.

10. L'Agence de l'Union européenne pour la cybersécurité (ENISA) devrait dresser un inventaire complet des menaces propres aux réseaux 5G. Le groupe de coopération et le réseau des centres de réponse aux incidents de sécurité informatique institué par la directive (UE) 2016/1148 devraient appuyer ce processus.

11. En tenant compte de tous ces éléments et au plus tard le 1er octobre 2019, les États membres devraient mener à bien, avec le soutien de la Commission et en association avec l'ENISA, un examen conjoint de l'exposition, à l'échelle de l'Union, aux risques liés aux infrastructures qui sous-tendent l'écosystème numérique, en particulier les réseaux 5G.

12. Cet examen conjoint devrait accorder la priorité à une analyse des risques concernant les éléments particulièrement sensibles ou vulnérables qui sont au cœur des réseaux 5G, le centre d'exploitation et de maintenance ainsi que les éléments du réseau d'accès à la 5G utilisés dans des applications industrielles.

13. Dans un deuxième temps, cet examen conjoint devrait être étendu à d'autres éléments stratégiques de la chaîne de valeur numérique.

Une boîte à outils commune au niveau de l'Union pour faire face aux risques

14. Les travaux du groupe de coopération devraient viser à recenser les bonnes pratiques du type prévu au point 4 suivies au niveau national. Sur la base de ces bonnes pratiques nationales, une boîte à outils constituée de mesures de gestion des risques possibles appropriées, efficaces et proportionnées devant permettre d'atténuer les risques recensés en matière de cybersécurité au niveau national et au niveau de l'Union devrait être approuvée au plus tard le 31 décembre 2019 et devrait conseiller la Commission sur la mise au point d'exigences minimales communes contribuant à garantir un niveau élevé de cybersécurité des réseaux 5G dans l'ensemble de l'Union.

15. Cette boîte à outils devrait comprendre:

a) un inventaire des types de risques en matière de sécurité susceptibles d'affecter la cybersécurité des réseaux 5G (par exemple risque lié à la chaîne d'approvisionnement, risque de vulnérabilité des logiciels, risque lié au contrôle d'accès, risque découlant du cadre juridique et politique auquel les fournisseurs d'équipement des technologies de l'information et de la communication peuvent être soumis dans les pays tiers); et

b) un train de mesures d'atténuation possibles (par exemple certification par des tiers du matériel, des logiciels ou des services, tests formels du matériel et des logiciels ou contrôles de conformité, processus visant à garantir l'existence et l'application des contrôles d'accès, recensement des produits, services ou fournisseurs jugés potentiellement non sûrs, etc.). Ces mesures devraient être valables pour tous les types de risques en matière de sécurité recensés dans un ou plusieurs États membres à l'issue de l'évaluation des risques.

16. Une fois que des systèmes européens de certification de cybersécurité applicables aux réseaux 5G auront été élaborés, les États membres devraient adopter, conformément au droit de l'Union, des réglementations techniques nationales prévoyant la certification obligatoire des produits, services ou systèmes des technologies de l'information et de la communication couverts par ces systèmes.

17. Les États membres, conjointement avec la Commission, devraient déterminer les conditions relatives à la sécurité des réseaux publics face aux accès non autorisés dont l'autorisation générale devrait être assortie, ainsi que les exigences de sécurité des réseaux dont le respect devrait faire l'objet d'engagements de la part des entreprises participant aux procédures de sélection pour l'octroi des droits d'utilisation des bandes de fréquences destinées aux réseaux 5G conformément à la directive 2002/20/CE. Ces exigences devraient être reflétées, si possible, dans les mesures visées au point 4 c).

18. Les États membres devraient coopérer avec la Commission pour établir des exigences de sécurité spécifiques qui pourraient s'appliquer dans le cadre des marchés publics liés aux réseaux 5G. Parmi elles, devraient figurer, entre autres, des exigences obligatoires concernant la mise en œuvre de systèmes de certification de cybersécurité dans le cadre des marchés publics, dans la mesure où de tels systèmes ne sont pas encore contraignants pour tous les fournisseurs et tous les opérateurs.

V. **EXAMEN**

19. Les États membres devraient coopérer avec la Commission pour évaluer les effets de la présente recommandation avant le 1er octobre 2020 en vue de déterminer la marche à suivre. Cette évaluation devrait tenir compte du résultat de l'évaluation coordonnée des risques au niveau de l'Union et de la boîte à outils de l'Union.

Fait à Strasbourg, le 26 mars 2019.

Par la Commission

Julian KING

Membre de la Commission