Conseil de
l'Union européenne

Bruxelles, le 2 décembre 2020
(OR. en)

13629/20

CYBER 263
TELECOM 248
COPEN 362
CODEC 1266
COPS 441
COSI 235
CSC 344
CSCI 86
IND 248
RECH 493
ESPACE 77

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	2 décembre 2020
Destinataire:	délégations
Objet:	Conclusions du Conseil sur la cybersécurité des dispositifs connectés - Conclusions du Conseil approuvées par procédure écrite

Les délégations trouveront en annexe les conclusions du Conseil sur la cybersécurité des dispositifs connectés, approuvées par le Conseil par procédure écrite le 2 décembre 2020.

ANNEXE

Conclusions du Conseil sur la cybersécurité des dispositifs connectés

Le Conseil de l'Union européenne,

RAPPELANT:

- les conclusions du Conseil sur la communication conjointe au Parlement européen et au Conseil: "Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide",
- les conclusions du Conseil sur le renforcement des capacités en matière de cybersécurité dans l'UE,
- les conclusions du Conseil sur l'importance de la 5G pour l'économie européenne et sur la nécessité d'atténuer les risques pour la sécurité liés à la 5G,
- les conclusions du Conseil sur l'avenir d'une Europe fortement numérisée après 2020: "Stimuler la compétitivité numérique et économique dans l'ensemble de l'Union et la cohésion numérique",
- les conclusions du Conseil intitulées "Façonner l'avenir numérique de l'Europe",
- les conclusions du Conseil européen sur la COVID-19, le marché unique, la politique industrielle, le numérique et les relations extérieures,
- la communication de la Commission européenne intitulée "Façonner l'avenir numérique de l'Europe";

1. MET EN EXERGUE le fait que l'Union européenne et ses États membres doivent assurer leur souveraineté numérique et leur autonomie stratégique, tout en préservant une économie ouverte. Cela suppose notamment de renforcer la capacité à faire des choix technologiques autonomes et de disposer, parmi les principaux piliers, d'infrastructures, de produits et de services résilients et sûrs pour instaurer la confiance sur le marché unique numérique et au sein de la société européenne. Les valeurs fondamentales de l'Union européenne préservent en particulier la vie privée, la sécurité, l'égalité, la dignité humaine, l'état de droit et un internet ouvert, qui sont autant de conditions préalables à l'avènement d'une société, d'une économie et d'une industrie fondées sur le numérique et axées sur l'humain;

2. MESURE l'importance croissante des dispositifs connectés et de leur sécurité, y compris en ce qui concerne les machines, capteurs et réseaux qui constituent l'internet des objets (IDO). Les dispositifs connectés joueront un rôle clé dans la poursuite du façonnement de l'avenir numérique de l'Europe, du point de vue industriel et commercial, ainsi que dans la vie quotidienne des consommateurs d'une nouvelle génération de technologies. En plus de la 5G, l'intelligence artificielle, l'informatique quantique, le calcul à haute performance, l'informatique en nuage, les technologie des registres distribués, à savoir la chaîne de blocs et toute autre nouvelle application ou possibilité favorisant une croissance économique durable et un niveau de numérisation plus élevé de notre société ne peuvent être mis en œuvre que par des dispositifs connectés et cybersécurisés;

3. NOTE que l'utilisation accrue de produits de consommation et de dispositifs industriels connectés à l'internet fera également peser de nouveaux risques sur la vie privée, la sécurité de l'information et la cybersécurité, y compris et de plus en plus par des effets potentiels sur l'intégrité et la disponibilité des produits et des données, ce qui peut avoir une incidence directe sur la sécurité. Il est essentiel de réduire autant que possible ces risques afin de protéger les consommateurs, de renforcer la cyber-résilience globale de l'Europe et d'affermir la confiance des citoyens à l'égard des solutions et technologies numériques. Cela favorisera également la compétitivité et les capacités d'innovation des fournisseurs européens de tels dispositifs. La cybersécurité et le respect de la vie privée devraient être reconnus comme des exigences essentielles pour les processus d'innovation, de production et de développement des produits, y compris la phase de conception (sécurité dès le stade de la conception), et devraient être assurés tout au long du cycle de vie d'un produit et de sa chaîne d'approvisionnement;

4. MET EN AVANT le fait qu'en plus d'assurer un niveau élevé de sécurité des dispositifs connectés, il est tout aussi important de sensibiliser davantage les consommateurs à leurs risques potentiels pour la vie privée et la sécurité. Cela contribuerait à atténuer autant que possible les menaces découlant d'une utilisation accrue des dispositifs connectés, à renforcer la confiance dans le marché unique numérique et à tirer le meilleur parti des avantages économiques et sociétaux qu'offrent les technologies des dispositifs connectés;

5. SOULIGNE que les investissements publics dans la recherche et l'innovation, notamment dans le cadre d'Horizon Europe et du programme pour une Europe numérique, ainsi que les investissements privés, pourraient créer de précieuses incitations à rendre les dispositifs connectés plus sûrs et plus sécurisés, et donc à rendre les réseaux de communication intelligents plus résilients. Il convient également d'accélérer les investissements dans les infrastructures et technologies numériques nécessaires au déploiement des plus récentes technologies des dispositifs connectés, afin de parvenir à une position de premier plan dans les domaines industriel et numérique et d'assurer l'autonomie stratégique, tout en préservant une économie ouverte;

6. MET L'ACCENT sur la nécessité d'assurer un niveau de complémentarité et de comparabilité élevé des fonctionnalités de sécurité des systèmes informatiques et de leurs composants, qui sont utilisés dans de nombreux secteurs différents du marché unique numérique;

7. PREND ACTE des développements actuels au niveau de l'Union visant à relever le niveau de cybersécurité des dispositifs connectés, notamment en ce qui concerne les initiatives récentes de la Commission visant à traiter, à court terme, les aspects relatifs à la cybersécurité dans les actes juridiques pertinents, par exemple les actes relevant du nouveau cadre législatif (NCL), en particulier la directive 2014/53/UE (directive relative aux équipements radioélectriques). INSISTE sur le fait qu'il importe d'évaluer la nécessité d'une législation horizontale, précisant également les conditions nécessaires pour la mise sur le marché, sur le long terme, pour traiter tous les aspects pertinents de la cybersécurité des dispositifs connectés, tels que la disponibilité, l'intégrité et la confidentialité. SE FÉLICITE, à cet égard, de la tenue d'une discussion visant à examiner le champ d'application d'une telle législation et ses liens avec le cadre de certification de cybersécurité défini dans le règlement sur la cybersécurité (CSA), dans le but de relever le niveau de sécurité au sein du marché unique numérique;

8. ATTIRE L'ATTENTION SUR LE FAIT que les exigences en matière de cybersécurité devraient être définies conformément à la législation pertinente de l'Union, y compris le CSA, le NCL, le règlement relatif à la normalisation européenne et une éventuelle législation horizontale à venir, afin d'éviter toute ambiguïté et toute fragmentation de la législation;

9. EST CONSCIENT du rôle important joué par toutes les parties prenantes, en particulier les fabricants, afin d'élever le niveau de cybersécurité des dispositifs connectés au sein du marché unique numérique; RECOMMANDE en conséquence une coordination et une coopération étroite avec toutes les parties prenantes publiques et privées concernées, y compris dans la perspective d'une éventuelle législation horizontale future;

9 *bis*. SE FÉLICITE des travaux en cours menés par l'ENISA en vue d'élaborer les premiers schémas de certification de cybersécurité de l'UE, à savoir les critères communs de l'Union européenne proposés et les schémas applicables aux services en nuage proposés. Ces schémas constitueront un socle utile pour la certification des dispositifs connectés;

10. SOULIGNE que tout schéma de certification supplémentaire pour les dispositifs connectés et les services connexes qui serait prévu dans le programme de travail glissant de l'Union et défini dans le règlement sur la cybersécurité devrait préciser les moyens de se conformer aux exigences de sécurité applicables au niveau d'assurance pertinent sur la base de normes spécifiques européennes et reconnues au niveau international, indépendamment du secteur dans lequel le produit doit être utilisé, ainsi que les spécifications d'essai, les certificats, etc. qui devront être appliqués;

11. RECONNAÎT que la certification des dispositifs connectés nécessiterait des normes, des règles ou des spécifications techniques pertinentes pour les évaluations de cybersécurité au titre du règlement sur la cybersécurité. Par conséquent, INSISTE sur la nécessité d'établir des normes, des règles ou des spécifications techniques en matière de cybersécurité pour les dispositifs connectés et RECOMMANDE de renforcer les efforts déployés par les organisations européennes de normalisation en la matière. Parallèlement, NOTE que la norme EN 303 645 de l'ETSI en matière de cybersécurité pour les dispositifs grand public de l'internet des objets constitue un pas important dans cette direction;

12. INVITE la Commission à envisager une demande de schémas de certification de cybersécurité candidats pour les dispositifs connectés et les services connexes, sur la base du programme de travail glissant de l'Union en cours d'élaboration, en tenant le plus grand compte des schémas européens horizontaux de certification de cybersécurité en phase de développement. Des schémas de ce type, appliqués à titre volontaire, permettront aux fabricants de ces produits de promouvoir les produits présentant le niveau d'assurance évalué;

13. INVITE à organiser une discussion sur la manière dont l'objectif de cybersécurité pourrait être inscrit dans une future législation horizontale couvrant les risques de cybersécurité liés aux dispositifs connectés, et NOTE dans le même temps qu'il convient d'envisager l'adaptation des exigences essentielles des directives correspondantes du NCL, en fonction des besoins;

14. ENCOURAGE la Commission à évaluer également, si nécessaire, les réglementations sectorielles complémentaires qui devraient définir le niveau de cybersécurité à respecter par le dispositif connecté, afin de garantir que des exigences spécifiques en matière de sécurité et de protection de la vie privée sont mises en place pour les dispositifs de ce type qui présentent des risques de sécurité plus élevés;

15. SOULIGNE qu'il est nécessaire d'améliorer la qualité de vie et le bien-être des citoyens européens et de renforcer la confiance dans le marché unique numérique. La sécurité et la protection de la vie privée dans nos sociétés sont essentielles pour préserver les valeurs fondamentales de l'Union. Par conséquent, SOULIGNE qu'il convient de s'appuyer sur le cadre fourni par le règlement sur la cybersécurité pour harmoniser les exigences de sécurité, en fonction des différents niveaux d'assurance, dans tous les secteurs du NCL, afin d'éviter la fragmentation et les contrôles multiples d'exigences identiques et d'offrir des conditions de concurrence et d'innovation équitables dans toute l'Union européenne;

16. INVITE la Commission, l'Agence de l'Union européenne pour la cybersécurité (ENISA), le comité pour l'évaluation de la conformité et la surveillance du marché des télécommunications et le groupe européen de certification de cybersécurité (GECC) à participer activement à cette initiative visant à consolider le marché unique numérique et à renforcer la confiance dans les produits, services et processus TIC pour les dispositifs connectés en veillant à la protection de la vie privée et à la cybersécurité, et à contribuer à ce que le secteur de l'internet des objets de l'Union soit plus compétitif au niveau mondial en garantissant les normes les plus élevées en matière de résilience, de sécurité et de sûreté;

17. SOULIGNE, dans ce contexte, qu'il est nécessaire de soutenir les PME, qui constituent une composante essentielle de l'écosystème européen de cybersécurité, et ENCOURAGE les PME à participer à toutes les consultations publiques lancées ainsi qu'aux activités de normalisation afin de prendre en compte leur contribution précieuse et importante pour faire de la cybersécurité un objectif accessible ainsi qu'un avantage concurrentiel sur le marché européen;

18. NOTE que l'obligation de garantir la cybersécurité et le respect de la vie privée tout au long du cycle de vie d'un produit et de sa chaîne d'approvisionnement pourrait avoir des répercussions positives sur l'empreinte environnementale du secteur technologique en amenant les fabricants vers des processus de développement et de production intelligents et durables et en réduisant ainsi la quantité de déchets électroniques liés à l'élimination des dispositifs connectés.