Conseil de l'Union européenne

PRESSE
FR

NOTE D'INFORMATION[1]
Bruxelles, le 4 juin 2018

Conseil "Transports, télécommunications et énergie" (questions relatives aux télécommunications)
Luxembourg, 8 juin 2018

Présidence: Ivaïlo Moskovski, ministre bulgare des transports, des technologies de l'information et des communications

La **session débutera** à 10 heures.

Les ministres tiendront un débat d'orientation sur une proposition visant à actualiser les **règles en matière de protection de la vie privée dans le cadre des communications électroniques**. Ce débat a pour objectif de faire avancer les travaux sur la proposition en vue d'arrêter une position commune du Conseil.

Le Conseil devrait approuver une orientation générale concernant une proposition d'**acte législatif sur la cybersécurité**. Cette proposition vise à améliorer l'actuelle Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour en faire un **organe permanent, l'Agence de l'UE pour la cybersécurité,** ainsi qu'à créer, **à l'échelle de l'UE, un cadre de certification de cybersécurité pour les produits et services liés aux technologies de l'information et de la communication (TIC)**.

Les ministres tiendront un débat d'orientation sur un projet de directive visant à promouvoir la **réutilisation des informations du secteur public**. Ce débat orientera les travaux futurs sur cette proposition.

La présidence informera les ministres des derniers développements intervenus en ce qui concerne un **code des communications électroniques européen** et un mandat révisé pour l'**Organe des régulateurs européens des communications électroniques (ORECE)**. Elle présentera également aux ministres des informations actualisées sur le projet de règlement relatif à la **libre circulation des données à caractère non personnel.**

La Commission informera les ministres de l'état d'avancement du **marché unique numérique**.

Enfin, la future présidence autrichienne présentera son **programme de travail**.

Au cours d'un déjeuner de travail, les ministres débattront des instruments financiers numériques dans le contexte du cadre financier pluriannuel.

Conférence de presse: vers 17 heures

* * *

Conférences de presse et manifestations publiques par transmission vidéo

Transmission vidéo, téléchargeable en format "diffusion" (MPEG 4), et galerie de photos

[1] La présente note a été élaborée sous la responsabilité du service de presse.

Service de presse - Secrétariat général du Conseil
Rue de la Loi 175 - B-1048 BRUXELLES - Tél.: +32 (0)2 281 63 19
press.office@consilium.europa.eu - www.consilium.europa.eu/press

Vie privée et communications électroniques

Le Conseil tiendra un **débat d'orientation** sur une proposition visant à actualiser les **règles en matière de protection de la vie privée dans le cadre des communications électroniques**. Le projet de règlement vise à assurer un niveau élevé de protection de la vie privée, des communications et des données à caractère personnel dans le domaine des télécommunications électroniques. Il a aussi pour but de créer des conditions de concurrence équitables pour les fournisseurs de services divers et de garantir la libre circulation des données et services de communications électroniques dans l'UE. Il remplacera la directive "vie privée et communications électroniques" actuellement en vigueur, qui a été mise à jour pour la dernière fois en 2009, et il complétera le règlement général sur la protection des données, qui s'applique depuis le 25 mai.

Le document préparé par la présidence à l'intention du Conseil contient également un **rapport sur l'état d'avancement** des discussions techniques menées au sein du Conseil.

En vertu de la proposition de la Commission sur la vie privée et les communications électroniques, la confidentialité des communications s'appliquerait au contenu de la communication comme aux métadonnées - par exemple, le destinataire de l'appel, l'heure et la localisation de l'appel ainsi que les sites web visités. La proposition contient par ailleurs des règles plus rigoureuses concernant les pourriels et les communications commerciales.

Le champ d'application des règles de protection de la vie privée serait étendu pour couvrir non seulement les télécommunications traditionnelles mais aussi les fournisseurs de nouveaux services tels que la voix sur IP ou les applications de messagerie instantanée et le webmail.

Le consentement serait requis pour avoir accès à des informations sur le dispositif de l'utilisateur. En vertu de nouvelles règles relatives aux cookies, le consentement serait exprimé au niveau du navigateur afin que les utilisateurs aient davantage la maîtrise de leurs dispositifs. Aucun consentement ne serait nécessaire pour les cookies ne portant pas atteinte à la vie privée qui améliorent l'expérience sur l'internet, tels que les historiques des paniers d'achat.

Au sein du Conseil, le groupe a réalisé des progrès considérables sur la proposition. Parmi les principales questions abordées lors des discussions figurent les liens entre les règles en matière de vie privée et de communications électroniques et le règlement général sur la protection des données, le traitement autorisé des métadonnées et les obligations incombant aux fournisseurs de logiciels concernant les paramètres de confidentialité. Néanmoins, les travaux doivent encore se poursuivre avant que le Conseil soit en mesure d'arrêter sa position. Afin de progresser en vue de la réalisation de cet objectif, la présidence demande aux ministres de fournir des **orientations** sur les éléments suivants:

- Pensez-vous que l'approche actuelle proposée par la présidence en ce qui concerne le **traitement** autorisé **des métadonnées** constitue une base acceptable pour avancer? Quelles autres améliorations pourraient être apportées?
- L'approche relative à la **protection des équipements terminaux et aux paramètres de confidentialité** constitue-t-elle une base acceptable pour avancer?
- Pensez-vous que le dernier texte de compromis proposé par la présidence permette de promouvoir la **compétitivité de l'industrie européenne** en fournissant des services innovants tout en préservant la **confidentialité des communications des citoyens et la protection de leurs données** (ou des données sensibles)?

Comment le texte acquerra-t-il force de loi? Pour être adopté, le texte devra être approuvé à la fois par le Conseil et par le Parlement européen. Le Parlement a adopté son mandat de négociation en octobre 2017.

Le marché unique numérique en Europe

Agence pour la cybersécurité et certification de cybersécurité

Le Conseil devrait arrêter sa position, dite "**orientation générale**", sur une proposition qui vise à améliorer l'actuelle Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour en faire un **organe permanent, l'Agence de l'UE pour la cybersécurité**, ainsi qu'à créer, **à l'échelle de l'UE, un cadre de certification de cybersécurité pour les produits et services TIC** (proposition de la Commission; projet d'orientation générale du Conseil).

La proposition, également dénommée **acte législatif sur la cybersécurité,** s'inscrit dans le paquet "cybersécurité" que la Commission a présenté en septembre 2017. Elle vise à atteindre un niveau élevé de cybersécurité et de cyber-résilience dans l'UE, ainsi qu'à renforcer la confiance envers les produits fondés sur les TIC et à améliorer le fonctionnement du marché intérieur.

Agence de l'UE pour la cybersécurité

L'Agence de l'UE chargée de la sécurité des réseaux et de l'information (ENISA) a été établie en Grèce en 2004, et son mandat actuel vient à échéance en 2020. L'ENISA fait office de centre d'information et de connaissance chargé de renforcer la sécurité des réseaux et de l'information dans l'UE et d'aider les États membres à se doter de moyens.

Les défis en matière de cybersécurité auxquels est confrontée l'UE ont évolué et se sont considérablement aggravés depuis que le mandat de l'ENISA a été défini, en 2013. En outre, le premier acte législatif de l'UE sur la cybersécurité adopté en 2016, à savoir la directive concernant la sécurité des réseaux et des systèmes d'information, prévoyait que l'ENISA joue un rôle central en soutien à sa mise en œuvre.

La proposition donnera à l'ENISA un mandat permanent et clarifiera son rôle en tant qu'agence de l'UE pour la cybersécurité. Elle lui confierait de nouvelles tâches pour apporter un soutien aux États membres, aux institutions de l'UE et aux autres parties prenantes sur les questions de cybersécurité. Elle serait chargée par exemple d'organiser des exercices de cybersécurité au niveau de l'UE et d'accompagner et de de promouvoir la politique de l'UE en matière de certification de cybersécurité.

Certification de cybersécurité à l'échelle de l'UE

La certification de cybersécurité a pour finalité de fournir des motifs de confiance aux utilisateurs en ce qui concerne les propriétés des produits et services TIC en matière de sécurité. Les informations relatives aux propriétés en matière de sécurité revêtent une importance croissante parce que la numérisation et la connectivité accrues ont entraîné une augmentation des risques en matière de cybersécurité. Cette tendance devrait se maintenir sous l'effet de l'essor rapide des objets connectés (l'"internet des objets"), des voitures connectées aux dispositifs de surveillance médicale en passant par les appareils électroménagers intelligents.

Aujourd'hui, plusieurs régimes de certification de sécurité différents existent dans l'UE. Par conséquent, il n'est pas exclu qu'une entreprise, pour pouvoir proposer ses produits sur plusieurs marchés, doive se soumettre à de multiples procédures, souvent coûteuses, dans différents pays de l'UE.

Afin de lutter contre la fragmentation du marché et de rendre les informations plus transparentes, le règlement proposé vise à mettre en place un cadre et un mécanisme permettant d'établir des systèmes de certification spécifiques pour des produits et des services TIC spécifiques, à savoir les "systèmes européens de certification de cybersécurité". Dans le cadre de ces régimes, un organisme tiers indépendant évaluerait un produit ou un service sur la base d'un ensemble défini de critères et délivrerait un certificat. Ceux-ci seront valables dans tous les pays de l'UE, ce qui permettrait aux consommateurs de mieux comprendre les propriétés en matière de sécurité d'un produit ou service, et aux entreprises d'exercer plus facilement leur activité par-delà les frontières.

Les propriétés en question seraient notamment la capacité de protéger les données contre le stockage non autorisé ou la perte ou l'altération accidentelles.

La certification serait facultative, sauf disposition contraire dans le droit de l'UE ou des États membres. Les systèmes feraient pleinement appel aux normes existantes, par exemple celles mises au point par les organisations européennes de normalisation.

La **proposition de compromis** de la présidence apporte un certain nombre de modifications à la proposition initiale. Par exemple, elle prévoit d'inclure les processus informatiques dans le champ d'application des systèmes de certification. Elle définit le rôle des États membres et du secteur privé dans la mise en place et l'élaboration de systèmes de certification. Elle crée également la possibilité pour les fabricants ou les fournisseurs de produits et de services TIC d'effectuer une auto-évaluation de conformité, quoiqu'uniquement en ce qui concerne les produits et les services à faible risque. De nouvelles dispositions ont été ajoutées en ce qui concerne le droit de déposer plainte et le droit à un recours juridictionnel effectif dans le cadre de la certification. En outre, un réseau d'agents de liaison nationaux serait créé afin de faciliter l'échange d'information entre l'ENISA et les États membres.

Le **Conseil européen** a insisté à plusieurs occasions sur l'importance que revêtent les mesures relatives à la cybersécurité de l'UE. Dans ses conclusions d'octobre 2017, il indiquait que "les propositions de la Commission concernant la cybersécurité devraient être présentées en temps utile et examinées sans retard, sur la base d'un plan d'action qui doit être établi par le Conseil". En mars dernier, il a invité l'UE et ses États membres à "continuer à renforcer leurs capacités de lutte contre les menaces hybrides".

Comment le texte acquerra-t-il force de loi? Le Conseil et le Parlement européen doivent tous deux marquer leur accord sur le texte avant qu'il puisse entrer en vigueur. Le Parlement n'a pas encore arrêté sa position.

Conclusions du Conseil: doter l'Union européenne d'une cybersécurité solide

Plan d'action mettant en œuvre les conclusions sur la cybersécurité

Communication conjointe - Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide

Réforme de la cybersécurité en Europe

Marché unique numérique en Europe

Site web de l'ENISA

Réutilisation des informations du secteur public

Le Conseil tiendra un **débat d'orientation** sur un projet de directive visant à **promouvoir la réutilisation des informations du secteur public**. La proposition vise à renforcer, dans l'UE, l'économie fondée sur les données en augmentant la quantité de données du secteur public disponibles à des fins de réutilisation, en assurant une concurrence équitable et en encourageant l'innovation transnationale fondée sur les données.

Le secteur public dans l'UE produit d'énormes quantités de données, telles que des données météorologiques, des cartes numériques et des statistiques. Ces informations constituent une ressource précieuse pour la société et l'économie. Depuis de nombreuses années, l'UE encourage donc les États membres à mettre à disposition le plus grand volume possible d'informations en vue de leur réutilisation.

Aux termes de la directive actuelle concernant la réutilisation des informations du secteur public, tout contenu qui est disponible en vertu des dispositions législatives nationales en matière d'accès aux documents peut, en principe, être réutilisé à des fins autres que l'objectif initial de la collecte, y compris à des fins commerciales. Cela s'applique aux institutions publiques aux niveaux national, régional et local, tels que les ministères, les organismes publics et les municipalités, ainsi qu'aux organisations qui sont essentiellement financées par les pouvoirs publics ou sous le contrôle de ces derniers. Les contenus que détiennent les musées, les bibliothèques et les archives sont également couverts, mais des règles spécifiques s'y appliquent.

Les redevances applicables en matière de réutilisation devraient, en principe, être limitées aux coûts marginaux de la demande, y compris les coûts de reproduction, de mise à disposition et de

diffusion, et les organismes du secteur public sont encouragés à appliquer des tarifs inférieurs, voire à pratiquer la gratuité totale.

La Commission a réexaminé la directive actuelle et propose d'actualiser les règles afin de tenir compte des évolutions technologiques et de remédier à un certain nombre de lacunes qui empêchent les petites et moyennes entreprises d'exploiter pleinement le potentiel des informations émanant du secteur public.

Les nouvelles règles proposées comportent l'obligation pour les organismes du secteur public de rendre les données dynamiques (par exemple les données "en temps réel" transmises par des capteurs ou des satellites) immédiatement disponibles grâce aux interfaces de programmation d'applications (API), pour un impact maximal. La proposition introduit aussi une catégorie spéciale d'ensembles de données de forte valeur, dont la réutilisation est associée à d'importants avantages socio-économiques. En principe, la réutilisation de ces ensembles de données de forte valeur devrait être gratuite.

La directive actualisée couvrirait aussi les données provenant de recherches financées par des fonds publics, qui devraient être mises à disposition sans qu'aucune redevance ne soit prélevée.

La Commission a présenté sa proposition en avril, en même temps que plusieurs autres initiatives liées aux données, qui visent à créer un espace européen commun des données afin de favoriser le développement de nouveaux produits et services fondés sur les données.

Le **débat d'orientation du Conseil** s'articulera autour d'un certain nombre de questions élaborées par la présidence dans un document d'information. Les questions sont les suivantes:

- Convenez-vous que la compétitivité de l'Europe requiert que des données publiques soient disponibles et constituent des ressources-clés pour l'innovation, les nouveaux produits et les applications liées à l'intelligence artificielle?
- Compte tenu du potentiel des informations du service public en tant que source d'innovation et de la rapidité de l'évolution technologique, convenez-vous qu'une politique européenne des données ouvertes devrait inclure, en particulier en ce qui concerne les organes et les domaines à englober, la possibilité de réutiliser les données dynamiques et la disponibilité d'ensembles de données de forte valeur en vue de leur réutilisation?

Les points de vue exposés par les ministres fourniront des orientations pour la suite des travaux du groupe du Conseil sur la proposition.

Comment le texte acquerra-t-il force de loi? Pour être adopté, le texte doit être approuvé à la fois par le Conseil et par le Parlement européen. Le Parlement n'a pas encore arrêté sa position.

Le marché unique numérique en Europe

Divers

- Directive sur le code des communications électroniques européen
- Règlement sur l'Organe des régulateurs européens des communications électroniques (ORECE)
  Informations communiquées par la présidence

  Code des communications électroniques
- Règlement concernant un cadre applicable à la libre circulation des données à caractère non personnel dans l'Union européenne.
  Informations communiquées par la présidence
- Marché unique numérique
  Informations communiquées par la Commission sur l'état d'avancement du dossier
- Programme de travail de la prochaine présidence
  Informations communiquées par la délégation autrichienne