Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 14/06/2013 - Document annexé à la procédure

Avis du Contrôleur européen de la protection des données sur : i) la communication conjointe de la Commission et de la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité intitulée «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé» et ii) sur la proposition de directive de la Commission concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union.

Le CEPD se félicite de la présentation d'une stratégie globale de cybersécurité et se réjouit du fait que la stratégie aille au-delà de l'approche traditionnelle consistant à opposer sécurité et respect de la vie privée en prévoyant une reconnaissance explicite du respect de la vie privée et de la protection des données en tant que valeurs essentielles.

Le CEPD constate toutefois que, du fait qu'elle ne prenne pas pleinement en considération d'autres initiatives parallèles de la Commission et d'autres procédures législatives en cours, comme la réforme de la protection des données et la proposition de règlement sur l'identification électronique et les services de confiance, la stratégie de cybersécurité **n'offre pas de vision véritablement complète et globale de la cybersécurité** au sein de l'Union et risque de perpétuer une approche fragmentée.

Le CEPD a formulé les recommandations suivantes :

Stratégie de cybersécurité :

- il serait judicieux de disposer d'une définition claire et restrictive de la «cybercriminalité» plutôt que d'une définition trop étendue ;
- la législation sur la protection des données devrait s'appliquer à toutes les actions de la stratégie, dès lors qu'elles concernent des mesures comprenant le traitement de données à caractère personnel ; c' est notamment le cas de nombreuses actions qui consistent en la mise en place de mécanismes de coopération ;
- en tant qu'organes de surveillance, les autorités chargées de la protection des données (APD) devraient dès être suffisamment associées à la mise en œuvre de mesures ayant trait au traitement de données à caractère personnel (comme le lancement du projet pilote de l'UE consacré à la lutte contre les réseaux zombies et les logiciels malveillants).

Directive sur la sécurité des réseaux et de l'information :

- introduire plus de clarté et de sécurité en dressant une liste exhaustive reprenant tous les acteurs du marché concernés, afin de garantir une approche pleinement harmonisée et intégrée de la sécurité au sein de l'UE;
- prévoir explicitement que la directive devrait s'appliquer sans préjudice des règles plus détaillées, existantes ou futures, dans des domaines spécifiques (comme celles qui seront définies concernant les fournisseurs de services de confiance dans la proposition de règlement sur l'identification électronique);
- ajouter un considérant pour expliquer la nécessité d'insérer la protection des données dès la conception et par défaut à un stade précoce de la conception des mécanismes établis dans la proposition ;
-

- préciser que le traitement des données à caractère personnel serait justifié dans la mesure où il est nécessaire pour atteindre les objectifs d'intérêt public poursuivis par la directive proposée ;
- définir les circonstances dans lesquelles une notification et préciser si la notification et ses documents justificatifs incluront ou non des détails sur les données à caractère personnel (comme les adresses IP) affectées par un incident de sécurité spécifique ;
- faire en sorte que l'exclusion des micro-entreprises du champ d'application de la notification ne s' applique pas aux acteurs qui jouent un rôle crucial dans la fourniture de services de la société de l' information, compte tenu notamment de la nature des informations qu'ils traitent (des données biométriques ou des données sensibles, par exemple);
- ajouter à la proposition des dispositions régissant l'échange ultérieur de données à caractère personnel par les autorités compétentes en matière de SRI avec d'autres destinataires, afin de garantir que les données ne soient divulguées qu'à des destinataires dont le traitement est nécessaire à l'accomplissement de leur mission ;
- définir le délai applicable à la conservation des données à caractère personnel;
- rappeler aux autorités compétentes leur obligation de fournir une information appropriée aux personnes concernées sur le traitement des données à caractère personnel, par exemple en publiant leur politique en matière de respect de la vie privée sur leur site web;
- ajouter une disposition relative au niveau de sécurité que les autorités compétentes en matière de SRI doivent respecter en ce qui concerne les informations collectées, traitées et échangées ;
- préciser que des critères relatifs à la participation des États membres au système sécurisé d'échange d'informations devraient assurer qu'un niveau élevé de sécurité soit garanti par tous les participants aux systèmes d'échange d'informations à toutes les étapes du traitement ;
- ajouter une description des rôles et responsabilités de la Commission et des États membres dans la création, l'exploitation et la maintenance du système sécurisé d'échange d'information ;
- préciser que tout transfert de données à caractère personnel vers des destinataires situés en dehors de l'UE doit être conforme à la directive 95/46/CE et au règlement (CE) n° 45/2001.