Résumé de l'avis du Contrôleur européen de la protection des données sur 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 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 texte complet de l'avis en anglais, français et allemand est disponible sur le site internet du CEPD http://www.edps.europa.eu)

(2014/C 32/10)

1. **Introduction**

1.1. *Consultation du CEPD*

1. Le 7 février 2013, la Commission et la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité ont adopté une communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé» [1] (ci-après la «communication conjointe», la «stratégie de cybersécurité» ou la «stratégie»).

2. Le même jour, la Commission a adopté une proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union [2] (ci-après la «directive proposée» ou la «proposition»). Cette proposition a été transmise au CEPD à des fins de consultation le 7 février 2013.

3. Avant l'adoption de la communication conjointe et de la proposition, le CEPD a eu la possibilité de formuler des commentaires non officiels à la Commission. Il se félicite que certains de ses commentaires aient été pris en considération dans la communication conjointe et dans la proposition.

4. **Conclusions**

74. Le CEPD se félicite que la Commission et la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité aient présenté une stratégie globale de cybersécurité assortie d'une proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information (SRI) dans l'UE. Cette stratégie vient compléter les actions politiques déjà mises en œuvre par l'Union dans le domaine de la sécurité des réseaux et de l'information.

75. Le CEPD 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 qui devraient inspirer la politique de cybersécurité dans l'UE et au niveau international. Le CEPD note que la stratégie de cybersécurité et la directive proposée sur la sécurité des réseaux et de l'information peuvent jouer un rôle fondamental en contribuant à garantir la protection des droits des personnes au respect de la vie privée et à la protection des données dans l'environnement en ligne. En même temps, il convient de veiller à ce qu'elles ne soient pas à l'origine de mesures qui constitueraient des atteintes illégales aux droits des personnes au respect de la vie privée et à la protection des données.

76. Le CEPD salue également le fait que la protection des données soit mentionnée dans plusieurs parties de la stratégie et qu'elle soit prise en considération dans la directive proposée sur la sécurité des réseaux et de l'information. Il regrette toutefois que ni la stratégie, ni la directive proposée ne soulignent davantage la contribution apportée par la législation existante et à venir en matière de protection des données à la sécurité et ne garantissent pleinement que toutes les obligations découlant de la directive proposée ou d'autres éléments de la stratégie soient complémentaires avec les obligations de protection des données et qu'elles ne se chevauchent pas, ni ne se contredisent.

77. Par ailleurs, le CEPD constate que, du fait qu'elle n'examine pas et 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

[1] JOIN(2013) 1 final.
[2] COM(2013) 48 final.

et compartimentée. Le CEPD note également que la directive proposée sur la sécurité des réseaux et de l'information ne permet pas encore une approche globale de la sécurité au sein de l'Union et que l'obligation prévue dans la législation sur la protection des données est probablement l'obligation de sécurité des réseaux et de l'information la plus complète dans le droit de l'UE.

78. Le CEPD déplore également que le rôle majeur joué par les autorités chargées de la protection des données dans la mise en œuvre et l'exécution des obligations de sécurité ainsi que dans le renforcement de la cybersécurité ne soit pas non plus dûment pris en considération.

79. En ce qui concerne la stratégie de cybersécurité, le CEPD met en lumière les éléments suivants:

— une définition claire des termes «cyber-résilience», «cybercriminalité» et «cyberdéfense» revêt une importance toute particulière dès lors que ces termes sont utilisés comme justifications pour certaines mesures spéciales susceptibles de porter atteinte aux droits fondamentaux, notamment les droits au respect de la vie privée et à la protection des données. Néanmoins, les définitions de la «cybercriminalité» fournies dans la stratégie et dans la convention sur la cybercriminalité restent très vagues. 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. Bien que la législation en matière de protection des données ne soit pas spécifiquement mentionnée dans les sections portant sur la cybercriminalité et la cyberdéfense, le CEPD souligne que bon nombre des actions prévues dans ces domaines sont susceptibles d'impliquer le traitement de données à caractère personnel et, partant, de relever du champ d'application de la législation applicable en matière de protection des données. Il constate également que de nombreuses actions consistent en la mise en place de mécanismes de coopération, lesquels exigeront la mise en œuvre de garanties adéquates de protection des données en ce qui concerne les modalités d'échange de données à caractère personnel;

— les autorités chargées de la protection des données (APD) jouent un rôle majeur dans le contexte de la cybersécurité. En tant que gardiennes des droits des personnes en matière de respect de la vie privée et de protection des données, les APD sont activement engagées dans la protection de leurs données à caractère personnel, que ce soit hors ligne ou en ligne. En tant qu'organes de surveillance, elles devraient dès lors 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). D'autres acteurs dans le domaine de la cybersécurité devraient également coopérer avec elles dans la réalisation de leurs tâches, par exemple dans l'échange de meilleures pratiques et dans les actions de sensibilisation. Le CEPD et les APD nationales devraient également participer de manière adéquate à la conférence de haut niveau qui se tiendra en 2014 pour évaluer les progrès accomplis dans la mise en œuvre de la stratégie.

80. En ce qui concerne la directive proposée sur la sécurité des réseaux et de l'information, le CEPD conseille aux législateurs:

— d'introduire plus de clarté et de sécurité à l'article 3, paragraphe 8, sur la définition des acteurs du marchés couverts par le champ d'application de la proposition et de dresser une liste exhaustive reprenant tous les acteurs concernés, afin de garantir une approche pleinement harmonisée et intégrée de la sécurité au sein de l'UE;

— de préciser à l'article 1er, paragraphe 2, point c), que la directive proposée s'applique aux institutions et organes de l'UE et d'ajouter une référence au règlement (CE) nº 45/2001 dans l'article 1er, paragraphe 5, de la proposition;

— de reconnaître un rôle plus horizontal pour cette proposition en ce qui concerne la sécurité, en prévoyant explicitement à l'article 1er qu'elle doit 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);

— d'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 et tout au long du cycle de vie des processus, procédures, organisations, techniques et infrastructures concernés, en tenant compte de la proposition de règlement sur la protection des données;

— de préciser les définitions de «réseau et système informatique» à l'article 3, paragraphe 1, et d'«incident» à l'article 3, paragraphe 4, et remplacer, à l'article 5, paragraphe 2, l'obligation d'élaborer un «plan d'évaluation des risques» par l'obligation d'«établir et maintenir un cadre de gestion des risques»;

— de préciser, à l'article 1er, paragraphe 6, que le traitement des données à caractère personnel serait justifié au titre de l'article 7, point e), de la directive 95/46/CE dans la mesure où il est nécessaire pour atteindre les objectifs d'intérêt public poursuivis par la directive proposée. Toutefois, il convient de veiller au respect des principes de nécessité et de proportionnalité afin que seules les données strictement nécessaires à la finalité à atteindre soient traitées;

— de définir à l'article 14 les circonstances dans lesquelles une notification est requise, ainsi que le contenu et le format de la notification, y compris les types de données à caractère personnel qui doivent être notifiées et 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 et, le cas échéant, dans quelle mesure. Il convient de tenir compte du fait que les autorités compétentes en matière de SRI ne devraient être autorisées à collecter et à traiter des données à caractère personnel dans le cadre d'un incident de sécurité que si cette collecte et ce traitement s'avèrent strictement nécessaires. La proposition devrait aussi fournir des garanties suffisantes pour veiller à la protection adéquate des données traitées par les autorités compétentes en matière de SRI;

— de préciser à l'article 14 que les notifications d'incident visées à l'article 14, paragraphe 2, devraient s'appliquer sans préjudice des obligations de notification des violations de données à caractère personnel imposées par la législation applicable en matière de protection des données. La proposition devrait exposer les principaux aspects de la procédure relative à la coopération des autorités compétentes en matière de SRI avec les APD dans les cas où un incident de sécurité implique une violation des données à caractère personnel;

— de modifier l'article 14, paragraphe 8, afin 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);

— d'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: i) les données à caractère personnel ne soient divulguées qu'à des destinataires dont le traitement est nécessaire à l'accomplissement de leur mission conformément à une base juridique appropriée; et ii) ces informations sont limitées au strict nécessaire à l'accomplissement de leur mission. Il convient également d'examiner la manière dont les entités qui fournissent des données au réseau de partage d'informations garantissent le respect du principe de la limitation de la finalité;

— de définir le délai applicable à la conservation des données à caractère personnel conformément aux objectifs définis dans la directive proposée, notamment en ce qui concerne la conservation par les autorités compétentes en matière de SRI et au sein de l'infrastructure sécurisée du réseau de coopération;

— de rappeler aux autorités compétentes en matière de SRI 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;

— d'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. Une référence aux exigences de sécurité visées à l'article 17 de la directive 95/46/CE devrait être spécifiquement introduite en ce qui concerne la protection des données à caractère personnel traitées par les autorités compétentes en matière de SRI;

— de préciser, à l'article 9, paragraphe 2, 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 et de résilience soit garanti par tous les participants aux systèmes d'échange d'informations à toutes les étapes du traitement. Ces critères devraient inclure des mesures appropriées de confidentialité et de sécurité conformément aux articles 16 et 17 de la directive 95/46/CE et aux articles 21 et 22 du règlement (CE) nº 45/2001. La Commission devrait être expressément tenue de respecter ces critères pour participer en tant que responsable du traitement au système sécurisé de partage d'informations;

— d'ajouter à l'article 9 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'informations, et de prévoir que la conception du système devrait être conforme aux principes de protection des données dès la conception et par défaut et de sécurité dès la conception; et

— de préciser à l'article 13 que tout transfert de données à caractère personnel vers des destinataires situés en dehors de l'UE doit être conforme aux articles 25 et 26 de la directive 95/46/CE et à l'article 9 du règlement (CE) n° 45/2001.

Fait à Bruxelles, le 14 juin 2013.

Peter HUSTINX

Contrôleur européen de la protection des données