Résumé de l'avis du Contrôleur européen de la protection des données relatif à la communication de la Commission européenne au Conseil et au Parlement européen concernant l'établissement d'un Centre européen de lutte contre la cybercriminalité

(Le texte complet de l'avis en anglais, français et allemand est disponible sur le site Internet du CEPD http://www.edps.europa.eu)

(2012/C 336/05)

1. Introduction

1.1. *Consultation du CEPD*

1. Le 28 mars 2012, la Commission a adopté une communication intitulée «Combattre la criminalité à l'ère numérique: établissement d'un Centre européen de lutte contre la cybercriminalité» ([1]).

2. Le CEPD constate que le Conseil a publié ses conclusions sur l'établissement d'un Centre européen de lutte contre la cybercriminalité les 7 et 8 juin 2012 ([2]). Le Conseil approuve les objectifs de la communication, appuie l'établissement du Centre (également appelé «EC3») au sein d'Europol et l'utilisation des structures existantes afin d'interagir avec d'autres domaines de la criminalité, confirme que l'EC3 servira de point focal dans la lutte contre la cybercriminalité et qu'il coopérera étroitement avec les agences et acteurs concernés au niveau international, et il exhorte la Commission, en concertation avec Europol, à développer davantage le champ des tâches spécifiques qui seront nécessaires pour rendre l'EC3 opérationnel d'ici à 2013. Toutefois, les conclusions ne parlent pas de l'importance des droits fondamentaux et, en particulier, de la protection des données lors de l'établissement de l'EC3.

3. Avant d'adopter la communication de la Commission, le CEPD a eu la possibilité de formuler des observations informelles sur le projet de communication. Dans celles-ci, le CEPD a souligné que la protection des données est un aspect essentiel à prendre en considération dans l'établissement du Centre européen de lutte contre la cybercriminalité (ci-après dénommé l'«EC3»). Malheureusement, la communication n'a pas tenu compte des observations formulées lors de cette étape informelle. De plus, le Conseil, dans ses conclusions, demande de s'assurer que le Centre soit déjà opérationnel dès l'année prochaine. C'est pourquoi la protection des données devrait être prise en compte dès les prochaines mesures adoptées à très court terme.

4. Cet avis traite de l'importance de la protection des données au moment de mettre en place l'EC3 et émet des suggestions spécifiques qui pourraient être prises en considération au cours de l'établissement du mandat de l'EC3 et lors de la révision législative du cadre juridique d'Europol. Le CEPD, agissant de sa propre initiative, a, par conséquent, adopté le présent avis sur la base de l'article 41, paragraphe 2, du règlement (CE) n° 45/2001.

1.2. *Champ d'application de la communication*

5. Dans sa communication, la Commission signale son intention de créer un Centre européen de lutte contre la cybercriminalité comme l'une des priorités de la stratégie de sécurité intérieure ([3]).

6. La communication énumère, de façon non exhaustive, plusieurs aspects de la cybercriminalité sur lesquels l'EC3 devrait se concentrer: les cybercrimes commis par des groupes criminels organisés, notamment ceux qui génèrent de grands bénéfices, tels que la fraude en ligne; les cybercrimes lourds de conséquences pour leurs victimes, tels que l'exploitation sexuelle des enfants en ligne; et les cybercrimes perturbant gravement les systèmes critiques de l'Union en matière de technologies de l'information et de la communication (TIC).

7. En ce qui concerne les fonctions du Centre, la communication mentionne quatre tâches principales ([4]):

— servir de point de convergence européen des informations relatives à la cybercriminalité;

— mettre en commun l'expertise européenne en matière de cybercriminalité pour soutenir les États membres dans le renforcement de leurs capacités;

([1]) La cybercriminalité n'est pas définie dans la législation de l'UE.
([2]) Conclusions du Conseil sur l'établissement d'un Centre européen de lutte contre la cybercriminalité, 3172e Conseil «Justice et Affaires Intérieures», Luxembourg, les 7 et 8 juin 2012.
([3]) La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre. COM(2010) 673 final du 22 novembre 2010. Voir également l'avis du CEPD relatif à cette communication, publié le 17 décembre 2010 (JO C 101 du 1.4.2011, p. 6).
([4]) Communication p. 4-5.

— apporter un soutien aux enquêtes des États membres sur la cybercriminalité;

— se faire le porte-voix des enquêteurs européens sur la cybercriminalité par l'intermédiaire des autorités policières et judiciaires.

8. Les informations traitées par l'EC3 seront recueillies auprès d'un *grand nombre de sources publiques, privées et libres,* enrichissant ainsi les données dont disposent les services de police, et elles *concerneraient les activités et méthodes de la cybercriminalité et les personnes suspectées.* L'EC3 collaborera aussi directement avec d'autres agences et organismes européens. Cela passera par la participation de ces entités au comité de direction de l'EC3, mais également, le cas échéant, par une coopération opérationnelle.

9. La Commission propose que l'EC3 devienne l'interface naturelle avec les activités d'Europol sur la cybercriminalité et d'autres unités internationales de police combattant la cybercriminalité. L'EC3 devrait également, en partenariat avec Interpol et d'autres partenaires stratégiques dans le monde, s'efforcer d'améliorer la coordination des réponses à la cybercriminalité.

10. En termes pratiques, la Commission propose de créer cet EC3 dans le cadre d'Europol. L'EC3 fera *partie d'Europol* ([1]) et, par conséquent, sera placé sous le régime juridique d'Europol ([2]).

11. Selon la Commission européenne ([3]), les principales nouveautés que l'EC3 proposé apportera aux activités actuelles d'Europol seront: i) des ressources accrues afin d'obtenir, de manière plus efficace, des informations auprès de différentes sources; ii) l'échange d'informations avec des partenaires hors services répressifs (provenant essentiellement du secteur privé).

1.3. *Objet principal de l'avis*

12. Le CEPD, dans cet avis, entend:

— demander à la Commission de clarifier la portée des activités de l'EC3, pour autant qu'elles sont pertinentes pour la protection des données;

— évaluer les activités prévues dans le contexte du cadre juridique actuel d'Europol, en particulier leur compatibilité avec le cadre;

— souligner les aspects importants pour lesquels le législateur devrait introduire d'autres détails dans le contexte de la future révision du régime juridique d'Europol afin de garantir un niveau plus élevé de protection des données.

13. L'avis est structuré de la manière suivante. Le point 2.1 explique pourquoi la protection des données est un élément indispensable dans la création de l'EC3. Le point 2.2 traite de la compatibilité des objectifs de l'EC3 définis dans la communication avec le mandat légal d'Europol. Le point 2.3 aborde la coopération avec le secteur privé et les partenaires internationaux.

3. **Conclusions**

50. Le CEPD considère la lutte contre la cybercriminalité comme une pierre angulaire du renforcement de la sécurité et de la sûreté dans l'espace numérique et de l'instauration de la confiance nécessaire. Le CEPD relève que la conformité avec les régimes de protection des données devrait être considérée comme faisant partie intégrante de la lutte contre la cybercriminalité et non comme un élément dissuasif pour son efficacité.

51. La communication évoque l'établissement d'un nouveau Centre européen de lutte contre la cybercriminalité au sein d'Europol, alors qu'un Centre de lutte contre la cybercriminalité d'Europol existait déjà depuis quelques années. Le CEPD souhaiterait davantage de clarté concernant les nouvelles capacités et les activités qui distingueront le nouvel EC3 du Centre de lutte contre la cybercriminalité d'Europol déjà existant.

([1]) Conformément aux recommandations de l'étude de faisabilité publiée en février 2012 évaluant les différentes options possibles (statu quo, hébergé à Europol, appartenant à/faisant partie d'Europol, centre virtuel). http://ec.europa.eu/home-affairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf

([2]) Décision 2009/371/JAI du Conseil datant du 6 avril 2009 portant création de l'Office européen de police (Europol).

([3]) Communiqué de presse du 28 mars. «Frequently Asked Questions: the new European Cybercrime Centre Reference»: MEMO/12/221 Date: 28.3.2012 http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/221

52. Le CEPD souligne que les compétences de l'EC3 doivent être clairement définies et pas seulement énoncées, en se référant au concept de «criminalité informatique» inclus dans la législation actuelle d'Europol. De plus, la définition des compétences et des garanties en matière de protection des données de l'EC3 devrait fait partie de la révision de la législation d'Europol. Jusqu'à ce que la nouvelle législation d'Europol soit applicable, le CEPD recommande que la Commission présente ces compétences et garanties en matière de protection des données dans le mandat du Centre. Pourraient y figurer:

— une définition claire des tâches de traitement de données (en particulier, enquêtes et activités de soutien opérationnel) dans lesquelles le personnel du Centre pourrait être engagé, seul ou en collaboration avec des équipes communes d'enquête;

— des procédures claires qui, d'une part, garantissent le respect des droits individuels (y compris le droit à la protection des données) et, d'autre part, garantissent que la preuve a été légalement obtenue et peut être utilisée en justice.

53. Le CEPD considère que les échanges de données à caractère personnel de l'EC3 avec un «*grand nombre de sources publiques, privées et libres*» impliquent des risques spécifiques en matière de protection des données, car ils donneront souvent lieu au traitement de données collectées à des fins commerciales et à des transferts internationaux de données. Ces risques sont pris en compte par la décision Europol actuellement en vigueur qui établit que, de manière générale, Europol ne doit pas échanger de données directement avec le secteur privé et, pour ce qui est des organisations internationales spécifiques, uniquement dans des circonstances bien concrètes.

54. Dans ce contexte, et compte tenu de l'importance de ces deux activités pour l'EC3, le CEPD recommande que des garanties appropriées de protection des données soient fournies conformément aux dispositions existantes dans la décision Europol. Ces garanties doivent être inscrites dans le mandat qui sera établi par l'équipe chargée de l'établissement de l'EC3 (et ultérieurement dans le cadre juridique révisé d'Europol) et ne doivent en aucun cas aboutir à un degré de protection des données moindre.

Fait à Bruxelles, le 29 juin 2012.

Peter HUSTINX

Contrôleur européen de la protection des données