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 CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1],

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[2],

vu la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008[3] relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale,

A ADOPTÉ L'AVIS SUIVANT:

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»[4].

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] JO L 350 du 30.12.2008, p. 60.
[4] La cybercriminalité n'est pas définie dans la législation de l'UE.

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 63
E-mail : edps@edps.europa.eu – Site web: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax: 02-283 19 50

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[5]. 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.[6]

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[7]:

[5] 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.
[6] 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 101/6.
[7] Communication p. 4-5.

- 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;
- 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*[8] et, par conséquent, sera placé sous le régime juridique d'Europol[9].

11. Selon la Commission européenne[10], 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.

[8] 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.

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

[10] Communiqué de presse du 28 mars. «Frequently Asked Questions: the new European Cybercrime Centre Reference»: MEMO/12/221 Date: 28/03/2012 http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/221.

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.

2. OBSERVATIONS

2.1. La protection des données comme élément indispensable dans la création du Centre

14. Le CEPD considère que la lutte contre la cybercriminalité est une pierre angulaire dans la consolidation de la sécurité et de la sûreté de l'espace numérique et dans l'instauration de la confiance nécessaire. Elle contribue également à renforcer la sécurité au sein de l'espace numérique et, par conséquent, améliore le niveau de protection des données dans cet espace. En effet, la protection des personnes dans le cyberespace tirera nécessairement avantage du fait que le Centre puisse atteindre ses objectifs tout en respectant pleinement les droits fondamentaux et notamment le droit à la protection des données. Dans ce contexte, le CEPD souhaite exprimer son soutien à la création de mécanismes de lutte contre la cybercriminalité, tels que le Centre proposé.

15. La lutte contre la cybercriminalité nécessitera souvent de traiter des données personnelles dans le cadre des enquêtes. Elle comporte donc des risques d'intrusions dans la vie privée des citoyens. C'est pourquoi les préoccupations relatives à la protection de la vie privée doivent être prises en considération, de même que les objectifs de l'EC3.

16. Le CEPD est persuadé qu'une action efficace pour lutter contre la cybercriminalité ne peut être mise en place sans l'appui d'un système valable de protection des données la complétant. Des dispositions appropriées sont nécessaires pour garantir que la surveillance et le traitement des données à caractère personnel ne seront exercés que de manière strictement ciblée, et que des mesures de sécurité adéquates empêcheront toute utilisation abusive de ce mécanisme. Le CEPD veut s'assurer que cette surveillance est effectuée dans un cadre clair moyennant la mise en place de garanties adéquates pour la protection des données.

17. Malheureusement, la communication ne mentionne pas la protection des données comme un élément à prendre en considération dans les activités du Centre. Le CEPD invite la Commission à reconnaître que les activités de l'EC3 devraient s'appuyer sur un système solide de protection des données et que cela devrait apparaître lors de sa mise en place, tant dans le mandat du Centre que dans la révision prochaine du cadre juridique d'Europol.

2.2. Compatibilité des objectifs de l'EC3 avec le mandat légal d'Europol

Du Centre de lutte contre la cybercriminalité d'Europol à l'EC3

18. Le CEPD relève qu'aucun instrument juridique particulier n'est prévu pour l'établissement de l'EC3. Il s'appuiera sur les structures existantes. Le Centre sera installé dans les locaux d'Europol et les activités de l'EC3 devront donc se conformer

aux dispositions de la décision du Conseil portant création d'Europol, y compris le cadre de protection des données d'Europol.

19. Europol a apporté son soutien aux États membres dans leur lutte contre la cybercriminalité à partir de 2002 avec la création du centre de criminalité high tech d'Europol. Durant cette période, Europol a mis au point une plateforme européenne destinée à répondre aux besoins spécifiques des États membres en matière de lutte contre la cybercriminalité.

20. Conformément au rapport général sur les activités d'Europol en 2011[11], un Centre de lutte contre la cybercriminalité d'Europol a été créé en 2011 et il semble que, conformément aux résultats mentionnés dans le rapport, il a déjà apporté des contributions significatives en termes de lutte contre les activités de cybercriminalité[12]. Cela soulève la question de savoir ce qu'il y a de nouveau en termes d'activités et de tâches dans la communication de la Commission, puisqu'un Centre de lutte contre la cybercriminalité d'Europol fonctionne déjà à Europol depuis 2011.

21. La communication ne fait pas référence à ces activités précédemment existantes d'Europol et semble pointer la création d'une structure entièrement nouvelle au sein d'Europol. En ce sens, le CEPD plaide pour davantage de clarté concernant les nouvelles activités prévues pour l'EC3 et souhaite également une analyse d'impact en termes de protection des données.

Infractions qui feront l'objet d'enquêtes de l'EC3

22. Le CEPD note qu'il importe d'évaluer en quoi les objectifs définis dans la communication en ce qui concerne l'EC3 correspondent au cadre juridique actuel d'Europol et notamment à son mandat actuel.

23. L'article 4, paragraphe 1, de la décision Europol et l'annexe incluent la lutte contre la «criminalité informatique» comme relevant de la compétence d'Europol. Cependant, le concept de «criminalité informatique» n'est pas défini, ni dans la décision du Conseil ni dans tout autre instrument juridique de l'Union. Les notions de «criminalité informatique» et de «cybercriminalité» sont liées, mais pas nécessairement identiques. Il ne peut non plus aller de soi que toutes les missions que l'EC3 devrait effectuer sont couvertes par le mandat d'Europol.

24. En l'absence d'une définition juridique de la cybercriminalité dans la législation de l'UE, le CEPD estime qu'il est important de clarifier les compétences du Centre. Au minimum, il faudrait clarifier quels «types de criminalité informatique» feront l'objet d'une enquête. Par exemple, il faudrait établir si l'EC3 doit s'attaquer à certaines infractions figurant déjà dans le cadre juridique de l'Union ou pas:

[11] Rapport général sur les activités d'Europol en 2011, 10036/12, ENFOPOL 141, Bruxelles, 24 mai 2012.

12 «En 2011, Europol a soutenu de grandes opérations de lutte contre la cybercriminalité: Crossbill (malware) et Mariposa II (Butterfly bots). Dans le domaine de l'exploitation en ligne des enfants, Europol a soutenu l'opération 'Rescue' dans une tentative réussie de démantèlement d'un réseau international de délinquants sexuels sur mineurs. L'opération 'Icarus' est une autre de ces opérations impliquant 23 pays.» Voir p. 59 du rapport 2011 d'Europol pour plus d'information.

- la décision-cadre 2005/222/JAI du Conseil relative aux attaques visant les systèmes d'information[13] et la proposition de directive[14] qui remplacera cette décision-cadre. La décision-cadre couvre notamment l'accès illicite aux systèmes d'information, l'atteinte à l'intégrité d'un système ou l'atteinte à l'intégrité des données;
- la directive 2011/93/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie[15]. Elle couvre, par exemple, les images d'abus sexuel d'enfants propagées par l'usage des nouvelles technologies et par l'internet;
- la décision 2001/413/JAI du Conseil concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces. Elle couvre notamment le fait d'effectuer ou de faire effectuer, intentionnellement, un transfert d'argent dans le but de procurer un avantage économique illégal à la personne qui commet l'infraction ou à une tierce partie, en altérant, effaçant ou supprimant des données informatiques, en particulier des données permettant l'identification, ou perturbant le fonctionnement d'un logiciel ou d'un système informatique.

25. De plus, dans le cadre de la stratégie européenne de gestion de l'identité, la Commission travaille actuellement sur une proposition de criminalisation de l'usurpation d'identité. En outre, la Convention de Budapest sur la cybercriminalité[16], signée en 2001, énumère un certain nombre d'infractions, telles que les infractions contre la confidentialité, l'intégrité et la disponibilité de systèmes et de données informatiques; les infractions en matière informatique; les infractions en relation avec le contenu; les infractions liées aux atteintes à la propriété intellectuelle et aux droits voisins. Il convient de préciser si toutes ces infractions seront également couvertes.

26. Étant donné que l'instrument juridique qui fournira une base juridique pour les activités du Centre constitue le cadre juridique actuel d'Europol, qui est en cours de révision[17], le CEPD recommande que ce processus de révision prenne en considération, entre autres aspects, la définition des compétences de l'EC3.

27. De plus, le CEPD recommande qu'en attendant la mise en application d'un cadre juridique révisé, l'étendue des activités de l'EC3 soit au moins spécifiée sous la forme d'un mandat[18]. Celui-ci devrait être présenté avant le début des opérations de l'EC3 (selon la communication, d'ici la fin 2013) et devrait entre autres faire état des infractions qui relèveront des compétences de l'EC3 et de celles qui n'en relèveront pas.

---

[13] Décision-cadre 2005/222/JAI du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information, JO L 69 du 16.3.2005, p. 67-71.

[14] La proposition 2010/273 de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil fait actuellement l'objet d'une procédure législative ordinaire.

[15] Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, JO L 335 du 27.11.2011, p. 1-14.

[16] Convention sur la cybercriminalité, Budapest, 23 novembre 2001.
http://conventions.coe.int/Treaty/fr/Treaties/html/185.htm

[17] Conformément à l'article 88, paragraphe 2, du traité sur le fonctionnement de l'Union européenne, le Parlement européen et le Conseil, statuant par voie de règlements conformément à la procédure législative ordinaire, déterminent la structure, le fonctionnement, le domaine d'action et les tâches d'Europol. Le programme de travail de la Commission européenne pour 2012 inclut cette initiative législative au point 64.
http://ec.europa.eu/atwork/programmes/docs/cwp2012_annex_fr.pdf

[18] Conformément à l'article 37, paragraphe 9, point c), de la décision du Conseil portant création d'Europol, le conseil d'administration prend toute décision ou mesure d'application conformément à la présente décision.

Activités de soutien opérationnel de l'EC3

28. L'EC3 devrait, conformément à la communication, fournir un *«soutien opérationnel»* aux enquêtes sur la cybercriminalité, par exemple en encourageant la mise en place d'équipes communes d'enquête. L'une de ses tâches proposées est de *«fournir une assistance de haute qualité en termes d'analyse (installations, stockage, outils), ainsi qu'une expertise en matière de cryptage pour les enquêtes sur la cybercriminalité»*[19]. Un autre exemple donné dans la communication concerne le travail d'un analyste d'Europol, qui est parvenu *«à passer outre les dispositifs de sécurité»*[20] d'un système informatique lors d'une enquête passée.

29. La base juridique générale de l'article 88 du TFUE[21] définit les tâches d'Europol et fait l'objet d'un développement dans la décision Europol. L'article 5, paragraphe 2, de la décision Europol expose ses tâches avec plus de détails, notamment l'assistance aux États membres en les faisant bénéficier d'un soutien, de conseils et de recherches concernant *«l'analyse et les méthodes de police techniques et scientifiques, ainsi que les méthodes d'enquête»* et *«le soutien à apporter aux États membres dans leurs missions de collecte et d'analyse d'informations provenant de l'internet, pour les aider à détecter les actes délictueux facilités ou commis à l'aide de l'internet»*.

30. De plus, en vertu de l'article 6 de la décision du Conseil relative à Europol, le personnel d'Europol peut participer, à titre d'appui, aux équipes communes d'enquête, mais il lui est formellement interdit de prendre part à l'adoption d'aucune mesure coercitive.

31. Les fonctions d'Europol, telles que définies dans la décision du Conseil, se limitent, en règle générale, à assurer un soutien en termes de connaissance des bonnes pratiques et d'analyse d'informations. Toutefois, la limite entre les activités opérationnelles et les mesures d'assistance dans le contexte de la cybercriminalité n'est pas très claire; le fait de *«passer outre les dispositifs de sécurité»* d'un système informatique ou de fournir un *«soutien opérationnel»* peut, dans certains cas, aller au-delà de la fourniture d'assistance et de la mise à disposition de connaissances. Par conséquent, le CEPD recommande de:

    - déterminer très précisément, dans le contexte de la lutte contre la cybercriminalité, dans quelles activités d'appui opérationnel le personnel du Centre pourrait être engagé, et dans quelle mesure, seul ou en collaboration avec des équipes communes d'enquête;
    - définir des procédures claires d'engagement dans des activités de soutien opérationnel qui, d'une part, garantissent le respect des droits individuels et, en particulier, le droit à la protection des données, et qui, d'autre part, garantissent que la preuve a été légalement obtenue et pourrait être utilisée en justice.

Utilisation des technologies renforçant la protection de la vie privée

[19] Communication, p. 5.
[20] Ibid.
[21] L'article 88, paragraphe 1, prévoit que la mission principale d'Europol est d'appuyer et de renforcer l'action des autorités policières et des autres services répressifs des États membres ainsi que leur collaboration mutuelle dans la prévention de la criminalité grave affectant au moins deux États membres, du terrorisme et des formes de criminalité qui portent atteinte à un intérêt commun qui fait l'objet d'une politique de l'Union, ainsi que la lutte contre ceux-ci.

32. La mise en œuvre pratique des activités de l'EC3 s'appuiera probablement sur l'utilisation d'une infrastructure informatique avancée traitant des quantités considérables de données à caractère personnel en vue de soutenir les actions envisagées dans la communication. Les technologies renforçant la protection de la vie privée peuvent être considérées comme des instruments permettant de réaliser un équilibre adéquat entre la réalisation des objectifs de l'EC3 et le respect des droits des individus.

33. Le CEPD recommande vivement que l'infrastructure informatique soit au préalable soigneusement évaluée et que des mesures concrètes pour mettre en œuvre des technologies renforçant la protection des données soient prises en considération. Cette approche sera pleinement conforme à celle du «respect de la vie privée dès la conception» (*privacy by design*) prévue dans la proposition récente de la Commission en faveur de la révision du cadre relatif à la protection des données.[22] Cela est d'autant plus important dans le cas présent, compte tenu de la brièveté du délai prévu pour rendre le Centre opérationnel d'ici à 2013, et du fait qu'à ce moment-là, le cadre juridique révisé d'Europol ne sera très probablement pas encore applicable.

34. La mise en application du principe de «privacy by design» contribuera donc à garantir la proportionnalité des activités du Centre et à minimiser les interférences avec les droits fondamentaux.

2.3. Coopération de l'EC3 avec le secteur privé et les partenaires internationaux

35. Le chapitre 2, paragraphe 1, de la communication décrit l'objectif de l'EC3, qui est de devenir un point focal dans la lutte contre la cybercriminalité. En particulier, il établit que l'une des fonctions de l'EC3 consistera à rassembler des renseignements relatifs à la cybercriminalité provenant d'un *grand nombre de sources publiques, privées et libres, enrichissant ainsi les données dont disposent les services de police*. La communication indique que les informations recueillies concerneront aussi les personnes suspectées d'activités de cybercriminalité. Par conséquent, l'EC3 traitera les données à caractère personnel au sens de l'article 2, point a), de la décision 2008/977/JAI du Conseil[23] dans ce contexte.

36. Le CEPD relève que la décision Europol régit strictement l'échange de données à caractère personnel entre Europol et le secteur privé et, dans la plupart des cas, comme analysé ci-après, les échanges de données entre Europol et le secteur privé ne devraient avoir lieu que par l'intermédiaire des autorités répressives nationales.

37. Le CEPD analyse, dans ce chapitre, comment les restrictions juridiques imposées par la décision Europol devraient être appliquées dans la pratique par l'EC3.

Coopération avec le secteur privé

[22] Article 19 de la proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données. COM/2012/010 final - 2012/0010 (COD).

[23] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350 du 30.122008, p. 60 - 71.

38. La communication énonce qu'Europol collectera des données provenant de toute source disponible (privée, publique ou libre) afin d'enrichir les données des services de police. Le CEPD note avec inquiétude que cette approche est dans le droit fil de la tendance générale qui consiste à garantir que le principe de disponibilité des informations visant à accroître l'efficacité des instances chargées de faire appliquer la loi est atteint sans le contrepoids des principes de proportionnalité et de nécessité requis par l'article 8 de la Charte des droits fondamentaux de l'Union, l'article 8 de la CEDH et l'article 16 du TFUE.

39. La lutte contre la cybercriminalité devrait souvent impliquer la coopération du secteur privé, car la plupart des données pertinentes pour enquêter sur les actes de cybercriminalité sont stockées par des entités privées qui conservent les transactions et communications électroniques dans le cadre de leurs activités régulières ou en conformité avec des obligations juridiques particulières. Par exemple, les opérateurs de télécommunications conservent les données internet et télécom à des fins commerciales ou conformément à la directive sur la conservation des données.[24]

40. Il est évident que la lutte contre la cybercriminalité constitue une finalité sans rapport avec les activités commerciales menées par ces entreprises. Par conséquent, les questions relatives au caractère licite et compatible du traitement des données personnelles sont à prendre en considération, car la collecte et l'utilisation ultérieure des données connexes dans la lutte contre la cybercriminalité peut constituer une violation du droit à la protection des données à caractère personnel.

41. Le CEPD a, à différentes reprises, fait référence à la coopération avec le secteur privé dans les activités en matière de répression[25], en reconnaissant son caractère délicat. En particulier, le CEPD est préoccupé par les questions soulevées par la participation d'un acteur commercial, offrant un service spécifique, dans un domaine tel que l'application des lois où, en principe, seules les autorités compétentes sont supposées intervenir, dans les conditions prévues par la législation nationale.

42. De plus, la communication semble viser des interactions directes entre l'EC3 et le secteur privé. Toutefois, Europol et, par la suite, l'EC3 ne sont pas habilités à interagir directement avec des entités privées sans restrictions. L'article 25 de la décision du Conseil relative à Europol dispose qu'Europol est autorisée à traiter des informations, y compris des données à caractère personnel, émanant dans certaines conditions de parties privées, dans la mesure où cela est nécessaire à l'exécution légitime des missions lui incombant:

---

[24] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, JO L 105/54.

[25] Avis du Contrôleur européen de la protection des données du 23 juin 2008 sur la proposition de décision du Parlement européen et du Conseil instituant un programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication, JO C 2 du 7.12009, p. 2–6.
Avis du Contrôleur européen de la protection des données du 22 février 2010 sur les négociations menées actuellement par l'Union européenne sur un accord commercial anti-contrefaçon (ACTA), JO C 147 du 5.6.2010, p. 1–13.
Avis du Contrôleur européen de la protection des données du 7 octobre 2011 sur la neutralité de l'internet, la gestion du trafic et la protection de la vie privée et des données personnelles. JO C 34 du 8.2.2012, p. 1–17.
Avis du Contrôleur européen de la protection des données du 24 avril 2012 sur la proposition de décision du Conseil relative à la conclusion de l'accord commercial anti-contrefaçon entre l'Union européenne et ses États membres, l'Australie, le Canada, la République de Corée, les Etats-Unis d'Amérique, le Japon, le Royaume du Maroc, les Etats-Unis mexicains, la Nouvelle-Zélande, la République de Singapour et la Confédération suisse, publié dans www.edps.europa.eu.

- en vertu de l'article 25, paragraphe 3, point a), les données à caractère personnel émanant de parties privées constituées en vertu du droit d'un État membre peuvent être traitées par Europol uniquement si elles sont transmises par l'intermédiaire de l'unité nationale dudit État membre conformément à son droit national. Cet article interdit expressément à Europol de contacter directement des parties privées pour rechercher des informations;
- en vertu de l'article 25, paragraphe 3, point b), les données à caractère personnel émanant de parties privées constituées en vertu du droit d'un État tiers avec lequel Europol a conclu un accord de coopération peuvent être traitées uniquement si elles ont été transmises par l'intermédiaire du point de contact dudit État;
- en vertu de l'article 25, paragraphe 3, point c), les données à caractère personnel émanant de parties privées constituées en vertu du droit d'un État tiers avec lequel Europol n'a pas conclu d'accord de coopération ne peuvent être traitées que si la partie privée concernée figure sur une liste que le conseil d'administration d'Europol est autorisée à dresser, et si Europol et la partie privée concernée ont conclu un protocole d'accord sur la transmission d'informations, confirmant la licéité de la collecte et de la transmission et précisant que les données à caractère personnel ne peuvent être utilisées qu'aux fins de l'exécution légitime des missions d'Europol. L'article 25, paragraphe 6, précise qu'Europol ne peut prétendre traiter ces données que pour les inclure dans le système d'information d'Europol ou dans des fichiers de travail à des fins d'analyse ou dans d'autres systèmes visés dans cet article;
- en vertu de l'article 25, paragraphe 4, Europol peut traiter des données à caractère personnel provenant de sources accessibles au public.

43. En outre, une interaction directe avec des entités privées sera compliquée car elle serait soumise à des législations nationales et garanties procédurales différentes en fonction de l'État membre où l'entité privée est située (par exemple dans un pays où la divulgation d'un type particulier de données pourrait faire l'objet d'une autorisation judiciaire, alors que dans un autre pays, ce ne serait pas nécessaire).

44. Le CEPD relève que la restriction selon laquelle Europol peut uniquement traiter des données qui ont été obtenues précédemment par l'intermédiaire d'unités nationales simplifiera l'interaction et contribuera à protéger ces données, étant donné que les unités nationales devraient garantir que l'échange d'informations avec l'EC3 est légal et que les garanties adéquates sont mises en place conformément à la législation de chaque État membre. Le CEPD recommande donc que cette sauvegarde soit maintenue tant dans le mandat de l'EC3 que dans la révision du cadre juridique d'Europol.

Coopération avec les partenaires internationaux

45. La prévention d'actes de cybercriminalité nécessite souvent la collecte et le traitement de données provenant de différents pays (dont certains pourraient être en dehors de l'Union européenne). La communication précise que l'un des objectifs de l'EC3 est de se faire le porte-voix des enquêteurs européens sur la cybercriminalité par le biais des autorités policières et judiciaires, tel que mentionné dans le texte de la communication. Pour atteindre cet objectif, l'EC3 serait l'interface naturelle avec les activités d'Interpol sur la cybercriminalité et d'autres unités internationales de police combattant la cybercriminalité.

46. En principe, cette activité est conforme à l'article 23 de la décision du Conseil relative à Europol, qui stipule qu'Europol peut échanger des informations, y compris des données à caractère personnel, dans la mesure où cela est nécessaire à l'exécution légitime de ses missions auprès d'États tiers et de certaines organisations concrètes.

47. En particulier, en vertu de l'article 23, paragraphe 3, Europol peut recevoir et utiliser des données à caractère personnel fournies par des États et organisations tiers. En vertu de l'article 23, paragraphe 6, Europol est autorisée à transmettre des données à caractère personnel à des États et organisations tiers si les conditions suivantes sont remplies:
    - elle a obtenu le consentement de l'État membre qui, à l'origine, a transmis les données concernées à Europol;
    - lorsque cela est nécessaire, dans des cas individuels, aux fins de la prévention et de la lutte contre les infractions relevant de la compétence d'Europol;
    - quand Europol a conclu avec l'entité destinataire un accord permettant la transmission des données sur la base d'une évaluation du caractère adéquat du niveau de protection des données;
    - le directeur d'Europol peut autoriser des transmissions de données à caractère personnel après avoir évalué le caractère adéquat du niveau de protection de l'entité destinataire si la transmission des données est absolument nécessaire à la sauvegarde des intérêts essentiels des États membres concernés dans le cadre des objectifs d'Europol ou dans le but de prévenir un danger imminent lié à des infractions pénales ou terroristes.

48. Le CEPD constate que, selon ces dispositions, l'EC3 ne doit pas échanger de données à caractère personnel à moins que cela ne soit justifié dans des cas individuels et lorsque l'entité destinataire offre un niveau adéquat de protection des données. Ces conditions doivent également être appréciées à la lumière des règles d'application définies dans la décision 2009/934/JAI du Conseil régissant les relations d'Europol avec ses partenaires.

49. Dans ce contexte, et compte tenu de l'importance que l'échange d'informations, au niveau international, prend dans la lutte contre la cybercriminalité, le CEPD recommande de vérifier si les accords internationaux actuels signés par Europol permettent d'échanger les informations requises, dans les quantités et avec la vitesse prévues dans ce contexte. Le CEPD note également que le mandat à établir par l'équipe chargée de l'établissement de l'EC3 devrait porter spécifiquement sur la coopération internationale, puisqu'il s'agira de l'une des tâches principales de l'EC3 en tant que porte-voix des enquêteurs européens sur la cybercriminalité et point de convergence des informations pour 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.

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

(**signé**)

Peter HUSTINX
Le Contrôleur européen de la protection des données