Avis du Contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen et au Conseil — «La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre»

(2011/C 101/02)

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 la demande d'avis formulée conformément au règlement (CE) nº 45/2001 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], et notamment son article 41,

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

1. Le 22 novembre 2010, la Commission a adopté une communication intitulée «La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre» (ci-après «la communication») [3]. La communication a été envoyée au CEPD pour consultation.

2. Le CEPD se réjouit d'avoir été consulté par la Commission. Avant même l'adoption de la communication, il avait formulé des observations informelles sur le projet de texte, dont certaines ont été prises en compte dans la version finale de la communication.

Contexte de la communication

3. La stratégie de sécurité intérieure de l'UE (ci-après «la SSI»), abordée dans la communication, a été adoptée le 23 février 2010 sous la présidence espagnole [4]. Elle définit un modèle de sécurité européen qui combine entre autres une action relative à la coopération policière et judiciaire, la gestion des frontières et la protection civile, en tenant dûment compte des valeurs européennes communes, telles que les droits fondamentaux. Ses principaux objectifs sont:

— présenter au public les instruments existants de l'UE qui contribuent déjà à garantir la sécurité et la liberté des citoyens de l'UE et la valeur ajoutée apportée par une action de l'UE dans ce domaine;

— développer des outils et politiques communs en suivant une approche plus intégrée qui s'attaque aux causes de l'insécurité et non uniquement à ses effets;

— renforcer la coopération policière et judiciaire, la gestion des frontières, la protection civile et la gestion des catastrophes.

4. La SSI a pour objet de cibler les menaces et les défis les plus urgents pour la sécurité de l'UE tels que la grande criminalité et la criminalité organisée, le terrorisme et la cybercriminalité, la gestion des frontières extérieures de l'UE et le renforcement de la résilience aux catastrophes d'origine naturelle ou humaine. La stratégie prévoit des lignes directrices générales, des principes et des orientations sur la manière dont l'UE devrait réagir à ces problèmes et appelle la Commission à proposer des mesures en temps opportun pour mettre en œuvre la stratégie.

5. Il importe en outre d'évoquer dans ce contexte les récentes conclusions du Conseil «Justice et affaires intérieures» sur la création et mise en œuvre d'un cycle politique de l'UE pour lutter contre la grande criminalité internationale, adoptées les 8 et 9 novembre 2010 [5] (ci-après «les conclusions de novembre 2010»). Ce document fait suite aux conclusions du Conseil sur l'architecture de la sécurité intérieure, approuvées en 2006 [6], et appelle le Conseil et la Commission à définir une SSI globale basée sur les valeurs et principes communs de l'UE tels que réaffirmés dans la Charte des droits fondamentaux de l'UE [7].

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] COM(2010) 673 final.
[4] Doc. 5842/2/10.
[5] 3043e session du Conseil «Justice et affaires intérieures», 8-10 novembre 2010, Bruxelles.
[6] Doc. 7039/2/06 JAI 86 CATS 34.
[7] Le cycle politique de l'UE pour lutter contre la grande criminalité internationale, abordé dans les conclusions de novembre 2010, consiste en quatre étapes: 1) élaboration d'une politique sur la base d'une évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne (SOCTA UE), 2) définition de la politique et prise de décision à travers le recensement par le Conseil d'un nombre restreint de priorités, 3) mise en œuvre et suivi des plans d'action opérationnels annuels (PAO) et 4) au terme du cycle politique, évaluation approfondie qui servira de base au cycle politique suivant.

6. Parmi les orientations et les objectifs qui devraient guider la mise en œuvre de la SSI, les conclusions de novembre 2010 font référence à la réflexion sur une approche proactive et fondée sur le renseignement, une coopération rigoureuse entre les agences de l'UE, notamment en améliorant encore l'échange d'informations entre elles et la sensibilisation des citoyens à l'importance de ce qui est accompli par l'UE aux fins de leur protection. Par ailleurs, les conclusions appellent la Commission à élaborer avec les experts des agences concernées et des États membres un plan stratégique pluriannuel (ci-après «PSP») pour chaque priorité définissant la stratégie la plus appropriée pour faire face au problème. Elles invitent également la Commission à mettre au point, en consultation avec les experts des États membres et des agences de l'UE, un mécanisme indépendant pour évaluer la mise en œuvre du PSP. Le CEPD abordera ces questions ci-après dans le présent avis étant donné qu'elles sont étroitement liées entre elles ou qu'elles affectent la protection des données à caractère personnel, la vie privée et d'autres droits et libertés fondamentaux qui leur sont liés.

Contenu et objectif de la communication

7. La communication propose cinq objectifs stratégiques, tous liés à la protection de la vie privée et des données:

— perturber les réseaux criminels internationaux,

— prévenir le terrorisme et s'attaquer à la radicalisation et au recrutement,

— accroître le niveau de sécurité des citoyens et des entreprises dans le cyberespace,

— renforcer la sécurité par la gestion des frontières, et

— renforcer la résilience de l'Europe aux crises et aux catastrophes.

8. La *SSI en action* telle que proposée dans la communication soumet un programme commun à l'intention des États membres, du Parlement européen, de la Commission, du Conseil, des agences et d'autres acteurs, y compris la société civile et les autorités locales, et leur propose des façons de collaborer tous ensemble au cours des quatre prochaines années pour réaliser les objectifs de la SSI.

9. La communication s'appuie sur le traité de Lisbonne et reconnaît les orientations données par le programme de Stockholm (et son plan d'action), qui soulignent au chapitre 4.1 la nécessité d'une SSI globale basée sur le respect des droits fondamentaux, la protection internationale et l'État de droit. En outre, conformément au programme de Stockholm, l'élaboration, le contrôle et la mise en œuvre de la stratégie de sécurité intérieure devraient être une des tâches prioritaires du comité de coopération opérationnelle en matière de sécurité intérieure (COSI) créé en vertu de l'article 71 TFUE. Pour garantir l'exécution effective de la SSI, celle-ci devrait également couvrir les aspects liés à la sécurité d'une gestion intégrée des frontières et, le cas échéant, la coopération judiciaire dans les affaires pénales en rapport avec la coopération opérationnelle dans le domaine de la sécurité intérieure. Il importe également de mentionner à cet égard que le programme de Stockholm appelle à une approche intégrée de la SSI, qui devrait aussi tenir compte de la stratégie de sécurité extérieure élaborée par l'UE ainsi que d'autres politiques de l'Union, notamment celles qui concernent le marché intérieur.

Objectif de l'avis

10. La communication porte sur divers domaines politiques qui relèvent du concept de «sécurité intérieure» au sens large dans l'Union européenne ou ont une incidence sur celui-ci.

11. L'objectif du présent avis n'est pas d'analyser tous les domaines politiques et questions spécifiques couverts par la communication, mais:

— d'examiner les objectifs mêmes de la SSI proposés dans la communication dans la perspective particulière de la protection de la vie privée et des données et — de ce point de vue — de souligner les liens nécessaires avec d'autres stratégies actuellement débattues et adoptées au niveau de l'UE;

— de préciser un certain nombre de notions et de concepts de la protection des données qui devraient être pris en compte lors de la conception, de l'élaboration et de la mise en œuvre de la SSI au niveau de l'UE;

— d'émettre, lorsque cela peut être utile et approprié, des suggestions sur la façon de tenir compte au mieux des préoccupations liées à la protection des données lors de l'exécution des mesures proposées dans la communication.

12. Le CEPD procédera en mettant notamment en exergue les liens entre la SSI et la stratégie de gestion de l'information et les travaux sur le cadre complet de protection des données. Le CEPD se réfèrera en outre à des concepts tels que les meilleures techniques disponibles et le «respect de la vie privée dès la conception», l'évaluation d'impact sur la protection de la vie privée et des données et les droits des personnes concernées, qui ont une influence directe sur la conception et la mise en œuvre de la SSI. L'avis formulera également des observations sur une série de domaines politiques choisis tels que la gestion intégrée des frontières, y compris EUROSUR et le traitement de données à caractère personnel par FRONTEX, ainsi que d'autres domaines comme le cyberespace et le TFTP.

II. OBSERVATIONS GÉNÉRALES

La nécessité d'une approche plus complète, inclusive et «stratégique» des stratégies de l'UE liées à la SSI

13. Diverses stratégies de l'UE basées sur le traité de Lisbonne et le programme de Stockholm et affectant directement ou indirectement la protection des données sont actuellement débattues et proposées au niveau de l'UE. La SSI en fait partie et est étroitement liée à d'autres stratégies (qui ont été abordées dans de récentes communications de la Commission ou sont envisagées dans un avenir proche), telles que la stratégie de gestion de l'information de l'UE et le modèle européen d'échange d'informations, la stratégie pour la mise en œuvre de la Charte des droits fondamentaux de l'UE, la stratégie globale de protection des données et la politique antiterroriste de l'UE. Dans le présent avis, le CEPD accorde une attention particulière aux liens avec la stratégie de gestion de l'information et le cadre complet de protection des données basé sur l'article 16 TFUE, qui entretiennent des liens politiques tout à fait évidents avec la SSI du point de vue de la protection des données.

14. Toutes ces stratégies forment une «mosaïque» complexe de lignes directrices politiques, de programmes et de plans d'action étroitement liés entre eux, qui préconisent une approche globale et intégrée au niveau de l'UE.

15. De manière plus générale, cette approche consistant à «relier les stratégies», si elle est retenue dans les actions futures, montrerait qu'il existe une vision au niveau de l'UE en matière de *stratégies de l'UE* et que ces stratégies, ainsi que les communications récentes qui les développent, sont étroitement liées, ce qui est le cas, le programme de Stockholm étant leur point de référence commun à toutes. Elle donnerait également lieu à des synergies positives entre les différentes politiques relevant du domaine de la liberté, de la sécurité et de la justice, et éviterait toute répétition inutile d'activités et d'efforts dans ce domaine. Cette approche donnerait également lieu, et c'est tout aussi important, à une application plus efficace et plus cohérente des règles relatives à la protection des données dans le contexte de toutes les stratégies liées entre elles.

16. Le CEPD souligne qu'un des piliers de la SSI est la gestion efficace de l'information au sein de l'Union européenne, qui devrait reposer sur les principes de la nécessité et de la proportionnalité pour justifier le besoin d'échange d'informations.

17. En outre, ainsi qu'on peut le lire dans l'avis du CEPD sur la communication relative à la gestion de l'information ([8]), le CEPD souligne que toute nouvelle mesure législative qui faciliterait le stockage et l'échange de données à caractère personnel ne doit être proposée que si sa nécessité est prouvée par des faits concrets ([9]). Cette exigence légale doit être transformée en approche politique proactive lors de la mise en œuvre de la SSI. La nécessité d'une approche globale de la SSI conduit inévitablement aussi à la nécessité d'évaluer tous les instruments et outils existants en matière de sécurité intérieure avant d'en proposer de nouveaux.

18. À cet égard, le CEPD suggère également un usage plus fréquent de dispositions prévoyant une évaluation périodique des instruments existants, comme le prévoit la directive sur la conservation des données, qui est actuellement en cours d'évaluation ([10]).

La protection des données en tant qu'objectif de la SSI

19. La communication fait référence à la protection des données à caractère personnel au paragraphe intitulé «Une politique de sécurité fondée sur des valeurs communes», où elle mentionne que les instruments et les actions utilisés pour mettre en œuvre la SSI doivent être fondés sur des valeurs communes, notamment l'État de droit et le respect des droits fondamentaux consacrés dans la Charte des droits fondamentaux de l'UE. Dans ce contexte, elle déclare que «Si un contrôle efficace de l'application de la législation dans l'Union passe par un échange d'informations, nous devons aussi protéger la vie privée des intéressés et leur droit fondamental à la protection des données à caractère personnel les concernant».

20. Cette déclaration est encourageante. On ne saurait toutefois considérer qu'elle suffit à régler la question de la protection des données dans la SSI. La communication ne donne pas de plus amples détails sur la protection des données ([11]) et n'explique pas davantage comment le respect de la vie privée et la protection des données à caractère personnel seront garantis de manière pratique dans les actions mettant en œuvre la SSI.

([8]) Avis du 30 septembre 2010 sur la communication de la Commission au Parlement européen et au Conseil — «Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice».

([9]) Il s'agit d'une exigence légale; voir notamment l'arrêt du 2 novembre 2010 de la Cour de justice dans les affaires jointes C-92/09 et C-93/09. Dans des contextes plus spécifiques, le CEPD a aussi plaidé en faveur de cette approche dans d'autres avis sur des propositions législatives dans le domaine de la liberté, de la sécurité et de la justice: par exemple, l'avis du 19 octobre 2005 sur trois propositions concernant le système d'information Schengen de deuxième génération (SIS II); l'avis du 20 décembre 2007 sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives; l'avis du 18 février 2009 sur la proposition de règlement relatif à la création du système EURODAC pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (CE) n° […/…] (établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale présentée dans l'un des États membres par un ressortissant de pays tiers ou un apatride]; l'avis du 18 février 2009 sur la proposition de règlement établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale présentée dans l'un des États membres par un ressortissant de pays tiers ou un apatride); et l'avis du 7 octobre 2009 sur l'accès des services de répression à EURODAC.

([10]) 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, 13.4.2006,. 54).

([11]) La protection des données n'est mentionnée de manière plus spécifique que dans le cadre du problème posé par le traitement de données à caractère personnel effectué par FRONTEX.

21. D'après le CEPD, la communication *La SSI en action* devrait avoir notamment pour objectif une *protection* au sens large qui assurerait un équilibre *approprié* entre, d'une part, la protection des citoyens contre les menaces existantes et, d'autre part, la protection de leur vie privée et leur droit à la protection des données à caractère personnel. En d'autres termes, les considérations liées à la sécurité et à la vie privée doivent être prises avec le même sérieux lors de l'élaboration de la SSI, conformément au programme de Stockholm et aux conclusions du Conseil.

22. En bref, la garantie de la sécurité dans le respect total de la protection de la vie privée et des données doit être mentionnée comme un objectif essentiel de la stratégie de sécurité intérieure de l'UE. Cela doit se manifester dans toutes les actions entreprises par les États membres et les institutions de l'UE afin de mettre en œuvre la stratégie.

23. À cet égard, le CEPD renvoie à la communication (2010) 609 sur une approche globale de la protection des données à caractère personnel dans l'Union européenne ([12]). Le CEPD publiera prochainement un avis sur cette communication, mais il souligne d'ores et déjà qu'une SSI efficace ne peut être mise en place sans le soutien d'un cadre solide de protection des données qui le complète et qui garantit la confiance mutuelle et une meilleure efficacité.

III. NOTIONS ET CONCEPTS APPLICABLES À LA CONCEPTION ET À LA MISE EN ŒUVRE DE LA SSI

24. Il est clair que certaines actions découlant des objectifs de la SSI sont susceptibles d'accroître les risques pour la protection de la vie privée et des données des individus. Pour contrebalancer ces risques, le CEPD souhaite attirer en particulier l'attention sur certains concepts tels que le «respect de la vie privée dès la conception», l'évaluation d'impact sur la protection de la vie privée et des données, les droits des personnes concernées et les meilleures techniques disponibles (MTD). Tous ces concepts doivent être pris en compte dans la mise en œuvre de la SSI et peuvent contribuer utilement à des politiques plus respectueuses de la vie privée et davantage axées sur la protection des données dans ce domaine.

Respect de la vie privée dès la conception

25. Le CEPD a plaidé à diverses occasions et dans divers avis en faveur du concept de vie privée «intégrée» («respect de la vie privée dès la conception» ou «paramétrage par défaut»). Ce concept est actuellement développé tant pour le secteur public que pour le secteur privé et doit donc jouer également un rôle important dans le contexte de la sécurité intérieure de l'UE et le domaine de la police et de la justice ([13]).

26. La communication ne mentionne pas ce concept. Le CEPD suggère qu'il y soit fait référence dans les actions ciblées qui seront proposées et entreprises pour mettre en œuvre la SSI, notamment dans le contexte de l'objectif 4, «Renforcer la sécurité par la gestion des frontières», où il est clairement fait état d'une utilisation renforcée des nouvelles technologies aux fins des contrôles et de la surveillance frontaliers.

Évaluation d'impact sur la protection de la vie privée et des données

27. Le CEPD encourage la Commission à réfléchir — dans le cadre des travaux futurs sur la conception et la mise en œuvre de la SSI sur la base de la communication — à ce qu'il y a lieu d'entendre par une véritable «évaluation d'impact sur la protection de la vie privée et des données» dans le domaine de la liberté, de la sécurité et de la justice, et en particulier de la SSI.

28. La communication évoque des évaluations de menaces et de risques, ce dont il convient de se réjouir. Les évaluations d'impact sur la protection de la vie privée et des données ne sont toutefois mentionnées nulle part. Le CEPD pense que les travaux sur la mise en œuvre de la communication sur la SSI offrent une bonne occasion de développer ces évaluations d'impact sur la protection de la vie privée et des données dans le contexte de la sécurité intérieure. Le CEPD note que ni la communication, ni les lignes directrices de la Commission pour l'évaluation d'impact ([14]) ne détaillent cet aspect ni n'en font une exigence politique.

29. Le CEPD recommande dès lors de réaliser, lors de la mise en œuvre d'instruments futurs, une évaluation d'impact plus spécifique et rigoureuse sur la protection de la vie privée et des données, soit en tant qu'évaluation distincte, soit dans le cadre de l'évaluation d'impact générale sur les droits fondamentaux effectuée par la Commission. Cette évaluation d'impact devrait non seulement affirmer des principes généraux ou analyser des options politiques, comme c'est le cas actuellement, mais aussi recommander des garanties particulières et concrètes.

30. Par conséquent, des indicateurs et des caractéristiques spécifiques devraient être élaborés pour garantir que chaque proposition ayant une incidence sur la protection de la vie privée et des données dans le domaine de la sécurité intérieure de l'UE soit soumise à un examen détaillé portant notamment sur des aspects tels que la proportionnalité, la nécessité et le principe de la limitation des finalités.

31. De plus, il pourrait être utile dans ce contexte d'évoquer le point 4 de la recommandation sur la RFID ([15]), dans lequel la Commission appelle les États membres à veiller à ce que les entreprises, en collaboration avec les parties intéressées

([12]) Communication de la Commission au Parlement européen, au Conseil et au Comité économique et social européen sur une approche globale de la protection des données à caractère personnel dans l'Union européenne, COM (2010) 609.

([13]) Dans son avis sur la communication de la Commission sur le programme de Stockholm, le CEPD a recommandé que les concepteurs et les utilisateurs de systèmes d'information soient légalement obligés de développer et d'utiliser des systèmes conformes au principe de «respect de la vie privée dès la conception».

([14]) SEC(2009) 92, 15.1.2009.

([15]) C(2009) 3200 final, 12.5.2009.

de la société civile, élaborent un cadre d'évaluation d'impact sur la protection de la vie privée et des données. En outre, la résolution de Madrid, adoptée en novembre 2009 par la Conférence internationale des commissaires à la protection des données et de la vie privée, encourage la mise en œuvre d'évaluations d'impact sur la protection de la vie privée et des données avant celle de nouveaux systèmes et technologies d'information en vue du traitement de données à caractère personnel ou de modifications substantielles aux traitements existants.

Droits des personnes concernées

32. Le CEPD note que la communication n'aborde pas spécifiquement la question des droits des personnes concernées, qui constitue un élément vital de la protection des données et qui devrait avoir une incidence sur la conception de la SSI. Il est essentiel de veiller à ce que dans tous les différents systèmes et instruments concernant la sécurité intérieure de l'UE, les personnes concernées bénéficient des mêmes droits pour ce qui est de la manière dont leurs données à caractère personnel sont traitées.

33. Bon nombre des systèmes mentionnés dans la communication instaurent des règles particulières en ce qui concerne les droits des personnes concernées (en ciblant aussi des catégories de personnes telles que les victimes, les personnes suspectées d'activités criminelles ou les migrants), mais il existe de grandes variations entre les systèmes et instruments, sans justification probante.

34. Par conséquent, le CEPD invite la Commission à examiner plus attentivement la question de l'harmonisation, à brève échéance, des droits des personnes concernées dans l'UE dans le contexte de la SSI et de la stratégie de gestion de l'information.

35. Il convient d'accorder une attention particulière aux mécanismes de recours. La SSI doit garantir que, lorsque les droits de certains individus n'ont pas été pleinement respectés, les responsables du traitement prévoient des procédures de plainte qui soient facilement accessibles, efficaces et abordables.

Meilleures techniques disponibles

36. La mise en œuvre de la SSI s'appuiera inévitablement sur l'utilisation d'une infrastructure informatique qui soutiendra les actions envisagées dans la communication. Les meilleures techniques disponibles (MTD) peuvent être considérées comme des instruments permettant de réaliser un équilibre adéquat entre la réalisation des objectifs de la SSI et le respect des droits des individus. Dans le contexte actuel, le CEPD souhaite rappeler la recommandation qu'il a formulée dans de précédents avis ([16]) concernant la nécessité que la Commission définisse et encourage, avec les parties prenantes de l'industrie, des mesures concrètes en vue de l'application des MTD. Cette application suppose le stade de développement le plus efficace et avancé des activités et de leurs modes d'exploitation démontrant l'aptitude pratique de techniques particulières à fournir les résultats escomptés d'une manière efficace, dans le respect du cadre européen régissant la protection de la vie privée et des données. Cette approche est en tout point conforme à l'approche basée sur le «respect de la vie privée dès la conception» mentionnée ci-dessus.

37. Lorsque cela est pertinent et possible, des documents de référence devraient être rédigés afin de fournir des lignes directrices et apporter une plus grande sécurité juridique en vue de la mise en œuvre effective des mesures définies par la SSI. Cela pourrait également favoriser l'harmonisation de ces mesures entre les différents États membres. Enfin, et surtout, la définition des MTD respectueuses de la vie privée et de la sécurité facilitera le rôle de contrôle des autorités chargées de la protection des données en leur fournissant des références techniques conformes à la protection de la vie privée et des données adoptées par les responsables du traitement.

38. Le CEPD note également l'importance d'un alignement adéquat de la SSI sur les activités déjà menées au titre du septième programme-cadre pour la recherche et le développement et le programme-cadre «Sécurité et protection des libertés». Une vision commune sur la mise en place de MTD favorisera l'innovation sur le plan des connaissances et des capacités requises pour protéger les citoyens tout en respectant les droits fondamentaux.

39. Enfin, le CEPD met en avant le rôle que l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) peut jouer dans l'élaboration de lignes directrices et l'évaluation des capacités de sécurité requises pour garantir l'intégrité et la disponibilité des systèmes informatiques, mais aussi dans la promotion de ces MTD. À cet égard, le CEPD se réjouit de l'inclusion de l'Agence en tant qu'acteur clé dans l'amélioration des capacités pour faire face aux cyberattaques et lutter contre la cybercriminalité ([17]).

Précision des acteurs et de leurs rôles

40. Dans ce contexte, il convient de mieux préciser les acteurs qui font partie de l'architecture de la SSI ou y contribuent. La communication énumère divers acteurs et parties prenantes tels que les citoyens, le pouvoir judiciaire, les

([16]) Avis du CEPD de juillet 2009 sur les systèmes de transports intelligents et avis du CEPD de décembre 2007 sur la communication par RFID. Voir également le rapport annuel 2006 du CEPD, p. 48.

([17]) Le CEPD envisage d'adopter, encore en décembre 2010, un avis sur le cadre légal de l'ENISA.

agences de l'UE, les autorités nationales, la police et les entreprises. Les rôles et compétences spécifiques de ces acteurs devraient être mieux abordés dans les actions spécifiques qui seront proposées dans le cadre de la mise en œuvre de la SSI.

IV. OBSERVATIONS PARTICULIÈRES SUR LES DOMAINES POLITIQUES LIÉS À LA SSI

Gestion intégrée des frontières (GIF)

41. La communication fait référence au fait qu'avec l'entrée en vigueur du traité de Lisbonne, l'UE est mieux à même de tirer parti des synergies entre les politiques de gestion des frontières pour les personnes et les marchandises. En ce qui concerne la circulation des personnes, elle affirme que «l'Union peut envisager la gestion des migrations et la lutte contre la criminalité comme un double objectif de la stratégie de gestion intégrée des frontières». Ce document considère la gestion des frontières comme un moyen potentiellement puissant de perturber la grande criminalité et la criminalité organisée ([18]).

42. Le CEPD constate en outre que la communication décrit trois volets stratégiques: 1) une utilisation accrue des nouvelles technologies aux fins du contrôle aux frontières (SIS II, VIS, système d'entrée/sortie et programme d'enregistrement des voyageurs); 2) une utilisation accrue des nouvelles technologies de surveillance des frontières (système européen de surveillance des frontières, EUROSUR) et 3) une meilleure coordination entre les États membres par l'intermédiaire de FRONTEX.

43. Le CEPD souhaite rappeler, à l'occasion du présent avis, qu'il a demandé dans plusieurs avis précédents qu'une politique claire de gestion des frontières — respectant pleinement les règles relatives à la protection des données — soit établie au niveau de l'UE. Le CEPD pense que les travaux actuels sur la SSI et la gestion de l'information offrent de très bonnes occasions de prendre des mesures plus concrètes dans le sens d'une approche politique cohérente de ces domaines.

44. Le CEPD note que la communication ne fait pas seulement référence aux systèmes à grande échelle existants et à ceux qui sont susceptibles d'être mis en service dans un proche avenir (tels que SIS, SIS II et VIS), mais également — dans le même esprit — aux systèmes susceptibles d'être proposés par la Commission à l'avenir mais pour lesquels aucune décision n'a encore été prise (à savoir, le programme d'enregistrement des voyageurs (RTP) et le système d'entrée/sortie). Il convient de rappeler à cet égard que les objectifs et la légitimité de l'introduction de ces systèmes doivent encore être clarifiés et démontrés, notamment à la lumière des résultats des évaluations d'impact particulières effectuées par la Commission. Dans le cas contraire, la communication peut donner l'impression de devancer le processus décisionnel et par conséquent de ne pas tenir compte du fait que la décision finale d'introduire ou non le RTP et le système d'entrée/sortie dans l'Union européenne n'a pas encore été prise.

45. Le CEPD suggère dès lors d'éviter ce genre d'anticipations dans les travaux futurs sur la mise en œuvre de la SSI. Comme il a été indiqué précédemment, toute décision sur l'introduction de nouveaux systèmes à grande échelle portant atteinte à la vie privée ne devrait être prise qu'après une évaluation adéquate de tous les systèmes existants, dans le respect des principes de nécessité et de proportionnalité.

EUROSUR

46. La communication signale que la Commission présentera une proposition législative visant à instituer EUROSUR en 2011 pour contribuer à la sécurité intérieure et à la lutte contre la criminalité. Elle signale également qu'EUROSUR utilisera les nouvelles technologies développées à l'aide des projets de recherche et les activités financés par l'UE, tels que l'imagerie satellite destinée à détecter et à suivre des cibles aux frontières comme, par exemple, les bateaux rapides qui transportent des stupéfiants vers l'UE.

47. Dans ce contexte, le CEPD note qu'il n'est pas clairement établi si la proposition législative sur EUROSUR, qui doit être présentée par la Commission en 2011, prévoira aussi le traitement des données à caractère personnel dans le contexte d'EUROSUR et, si tel est le cas, dans quelle mesure. La Commission n'a pas adopté de position claire sur ce point dans la communication. Cette question est d'autant plus pertinente que la communication établit un lien clair entre EUROSUR et FRONTEX aux niveaux tactique, opérationnel et stratégique (voir les observations ci-dessous sur FRONTEX) et qu'elle préconise une étroite coopération entre les deux agences.

Le traitement des données à caractère personnel par FRONTEX

48. Le CEPD a publié le 17 mai 2010 un avis sur la révision du règlement FRONTEX ([19]) dans lequel il appelle à mener un véritable débat et une réflexion approfondie sur la question de la protection des données dans le contexte du renforcement des tâches existantes de FRONTEX et de la délégation de nouvelles responsabilités à celle-ci.

49. La communication évoque la nécessité d'accroître la contribution de FRONTEX aux frontières extérieures dans le cadre de l'objectif 4, «Renforcer la sécurité par la gestion des frontières». À ce propos, la communication indique que sur la base de l'expérience acquise et dans le contexte de

([18]) Communiqué de presse sur la stratégie de sécurité intérieure de l'UE en action — cinq étapes vers une Europe plus sûre, MEMO/10/598.

([19]) Avis du Contrôleur européen de la protection des données sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) nº 2007/2004 du Conseil portant création d'une Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'Union européenne (FRONTEX).

l'approche globale de l'UE en matière de gestion de l'information, la Commission considère que permettre à FRONTEX de traiter et d'utiliser ces informations, avec une portée limitée et en accord avec des règles bien définies de gestion des données à caractère personnel, contribuera de manière importante au démantèlement d'organisations criminelles. Il s'agit là d'une approche nouvelle par rapport à la proposition de la Commission sur la révision du règlement FRONTEX, qui est examinée actuellement par le Parlement européen et le Conseil, et qui ne disait mot du traitement des données à caractère personnel.

50. Dans ce contexte, le CEPD se réjouit du fait que la communication donne quelques indications quant aux circonstances dans lesquelles ce traitement pourrait s'avérer nécessaire (par exemple, analyse de risques, meilleures performances des opérations conjointes ou échange d'informations avec Europol). Plus particulièrement, la communication explique qu'à l'heure actuelle, les informations sur des criminels impliqués dans des réseaux de trafics — auxquels FRONTEX est confrontée — ne peuvent être utilisées par la suite à des fins d'analyse de risques ou pour mieux cibler de futures opérations conjointes. Qui plus est, les données pertinentes sur les criminels présumés ne parviennent pas aux autorités nationales compétentes ou à Europol en vue d'enquêtes supplémentaires.

51. Le CEPD note néanmoins que la communication n'évoque pas les débats en cours sur la révision du cadre légal de FRONTEX qui, comme il a été indiqué précédemment, aborde cette question afin d'apporter des solutions législatives. En outre, la formulation de la communication mettant l'accent sur le rôle de FRONTEX dans le contexte de l'objectif visant à démanteler les organisations criminelles peut être interprétée comme un élargissement du mandat de FRONTEX. Le CEPD suggère de tenir compte de ce point lors de la révision du règlement FRONTEX et de la mise en œuvre de la SSI.

52. Le CEPD attire aussi l'attention sur la nécessité de veiller à ce qu'il n'y ait pas de duplication de tâches entre Europol et FRONTEX. Dans ce contexte, le CEPD se réjouit que la communication recommande d'éviter la duplication de tâches entre ces deux agences. Cette question pourrait toutefois aussi être abordée plus clairement tant dans le règlement FRONTEX révisé que dans les actions mettant en œuvre la SSI qui prévoient une étroite coopération entre FRONTEX et Europol. Cet élément revêt une importance particulière du point de vue des principes de la limitation des finalités et de la qualité des données. Cette remarque s'applique aussi à la coopération future avec des agences telles que l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) ou le Bureau européen d'appui en matière d'asile.

L'utilisation de données biométriques

53. La communication n'aborde pas spécifiquement le phénomène actuel de l'utilisation accrue de données biométriques dans le domaine de la liberté, de la sécurité et de la justice, y compris dans les systèmes informatiques à grande échelle de l'UE et d'autres outils de gestion des frontières.

54. Le CEPD saisit donc cette occasion pour rappeler sa suggestion ([20]) de tenir sérieusement compte de cette question très sensible du point de vue de la protection des données lors de la mise en œuvre de la SSI, notamment dans le contexte de la gestion des frontières.

55. Le CEPD recommande également d'élaborer une politique claire et rigoureuse en matière d'utilisation de données biométriques dans le domaine de la liberté, de la sécurité et de la justice, sur la base d'une évaluation sérieuse et d'une appréciation au cas par cas de la nécessité de l'utilisation des données biométriques dans le contexte de la SSI, dans le respect intégral de certains principes fondamentaux de la protection des données tels que la proportionnalité, la nécessité et la limitation des finalités.

TFTP

56. La communication annonce que la Commission élaborera en 2011 une politique de l'UE relative à l'extraction et à l'analyse des données de messagerie financière détenues sur son territoire. Dans ce contexte, le CEPD renvoie à son avis du 22 juin 2010 sur le traitement et le transfert de données de messagerie financière de l'UE aux États-Unis aux fins du programme de surveillance du financement du terrorisme (TFTP II) ([21]). Toutes les remarques critiques exprimées dans cet avis sont tout autant valides et applicables dans le contexte des travaux prévus sur un cadre de l'UE relatif aux données de messagerie financière. Il convient par conséquent d'en tenir compte dans les discussions portant sur cette question. Une attention particulière doit être accordée à la proportionnalité de l'extraction et du traitement de volumes importants de données relatives à des personnes qui ne sont pas soupçonnées et à la question du contrôle efficace par des autorités indépendantes et par le pouvoir judiciaire.

Sécurité des citoyens et des entreprises dans le cyberespace

57. Le CEPD se réjouit de l'importance que la communication attache aux actions préventives au niveau de l'UE et est d'avis que le renforcement de la sécurité dans les réseaux informatiques est un facteur essentiel contribuant au bon fonctionnement de la société de l'information. Le CEPD soutient également les activités spécifiques qui visent à améliorer la capacité de réaction aux cyberattaques, développer les capacités répressives et judiciaires et mettre en place des partenariats avec l'industrie afin de donner des moyens d'action aux citoyens et aux entreprises. L'ENISA joue en outre un rôle positif en tant que facilitateur d'un grand nombre d'actions prévues au titre de cet objectif.

([20]) Voir notamment l'avis du CEPD sur la communication relative à la présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice cité à la note 8.

([21]) Avis du CEPD du 22 juin 2010 sur la proposition d'une décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (TFTP II).

58. La *SSI en action* ne donne toutefois pas plus de précisions sur les actions répressives envisagées dans le cyberespace, la manière dont ces activités pourraient mettre en danger les droits individuels et les garanties nécessaires. Le CEPD appelle à une approche plus ambitieuse sur les garanties appropriées. Cette approche devrait être exposée afin de protéger les droits fondamentaux de tous les individus, y compris de ceux susceptibles d'être affectés par des actions visant à contrecarrer d'éventuelles activités criminelles dans ce domaine.

V. **CONCLUSIONS ET RECOMMANDATIONS**

59. Le CEPD demande qu'un lien soit établi entre les diverses stratégies de l'UE et les communications lors du processus de mise en œuvre de la SSI. Cette approche doit être suivie d'un plan d'action concret soutenu par une appréciation concrète des besoins, qui devrait déboucher sur une politique globale, intégrée et bien structurée de l'UE sur la SSI.

60. Le CEPD profite également de l'occasion pour souligner l'importance de l'obligation légale d'effectuer une appréciation concrète de tous les instruments existants devant être utilisés dans le contexte de la SSI et de l'échange d'informations avant d'en proposer de nouveaux. À cet égard, l'inclusion de dispositions prévoyant des évaluations régulières de l'efficacité des instruments concernés est vivement recommandée.

61. Le CEPD suggère de tenir compte, lors de la préparation du plan stratégique pluriannuel demandé par les conclusions du Conseil de novembre 2010, des travaux en cours sur le cadre complet de protection des données basé sur l'article 16 TFUE, et en particulier de la communication (2009) 609.

62. Le CEPD formule un certain nombre de suggestions sur des notions et des concepts pertinents du point de vue de la protection des données, dont il convient de tenir compte dans le domaine de la SSI, tels que le respect de la vie privée dès la conception, l'évaluation d'impact sur la protection de la vie privée et des données et les meilleures techniques disponibles.

63. Le CEPD recommande que, lors de la mise en œuvre d'instruments futurs, une évaluation d'impact sur la protection de la vie privée et des données soit effectuée, soit en tant qu'évaluation distincte, soit dans le cadre de l'évaluation d'impact générale sur les droits fondamentaux effectuée par la Commission.

64. Le CEPD invite également la Commission à élaborer une politique plus cohérente et constante sur les conditions d'utilisation de données biométriques dans le domaine de la SSI et préconise une plus grande harmonisation des droits des personnes concernées au niveau de l'UE.

65. Enfin, le CEPD formule un certain nombre d'observations sur le traitement des données à caractère personnel dans le contexte de la gestion des frontières, effectué notamment par FRONTEX et éventuellement dans le cadre d'EUROSUR.

Fait à Bruxelles, le 17 décembre 2010.

Peter HUSTINX

Contrôleur européen de la protection des données