AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du Contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen et au Conseil intitulée — «La politique antiterroriste de l'UE: principales réalisations et défis à venir»

(2011/C 56/02)

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 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], et notamment son article 41,

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

1. Le 20 juillet 2010, la Commission a adopté une communication intitulée «La politique antiterroriste de l'UE: principales réalisations et défis à venir» [3]. Cette communication vise à fournir «les éléments essentiels d'une évaluation politique de la stratégie actuelle de l'UE visant à lutter contre le terrorisme» et constitue également un élément de la stratégie de sécurité intérieure [4]. Elle évalue les réalisations antérieures et trace le contour des lignes d'action et des défis à venir pour la politique antiterroriste de l'UE.

2. De nombreuses initiatives mentionnées dans la communication ont déjà fait l'objet d'avis ou d'observations spécifiques de la part du CEPD. Toutefois, cette communication présente une perspective stratégique globale et des orientations à long terme qui justifient que le CEPD y consacre un avis.

3. Le présent avis vise donc à contribuer à ce que des choix stratégiques plus fondamentaux soient opérés dans un domaine où l'utilisation des informations personnelles est à la fois indispensable, massive et un sujet particulièrement sensible.

4. Cet avis n'aborde pas la communication la plus récente de la Commission dans ce domaine, la communication intitulée «La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre», qui a été adoptée le 22 novembre 2010 [5]. Cette dernière sera analysée par le CEPD dans un avis distinct, qui remettra encore une fois en évidence la nécessité d'établir des liens clairs entre les différents documents.

5. Dans le présent avis, le CEPD analyse les différents éléments de la communication, tout en formulant des conseils et des recommandations visant à garantir le respect du droit fondamental à la protection des données à caractère personnel dans le domaine de la politique antiterroriste de l'UE, en particulier en ce qui concerne les défis à venir et les nouvelles orientations stratégiques.

II. ANALYSE DE LA COMMUNICATION ET DE SES ENJEUX POUR LA PROTECTION DES DONNÉES

6. La communication est fondée sur la structure de la stratégie de lutte contre le terrorisme adoptée par l'UE en 2005 [6] pour analyser tout d'abord les quatre grands axes de la politique antiterroriste de l'UE: la prévention, la protection, la poursuite et la réaction. Un chapitre spécifique est ensuite consacré à des questions horizontales, à savoir le respect des droits fondamentaux, la coopération internationale et le financement.

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] COM(2010) 386 final.
[4] Voir page 2 de la communication.
[5] COM(2010) 673 final.
[6] Doc. 14469/4/05 du 30 novembre 2005.

1. **Prévention, protection, poursuite et réaction, et la nécessité d'intégrer les principes de la protection des données**

7. La «prévention» englobe une large palette d'activités, qui vont de la prévention de la radicalisation et du recrutement aux moyens à mettre en œuvre face aux modalités d'utilisation de l'internet par les terroristes. Dans ce contexte, la communication classe parmi les principales réalisations la décision-cadre du Conseil relative à la lutte contre le terrorisme, adoptée en 2002 ([1]) et modifiée en 2008 ([2]).

8. La «protection» des personnes et des infrastructures constitue également un thème très vaste comportant des initiatives relatives à la sécurité aux frontières, à la sécurité des transports, au contrôle des précurseurs d'explosifs, à la protection des infrastructures critiques et au renforcement de la sûreté de la chaîne d'approvisionnement.

9. La «poursuite» comporte la collecte d'informations, la coopération policière et judiciaire, les mesures destinées à empêcher les terroristes d'agir et la lutte contre le financement du terrorisme. Les défis à venir dans ce domaine incluent la mise en place d'un cadre européen pour l'utilisation des dossiers passagers (données PNR) ([3]), l'utilisation de l'article 75 du TFUE pour élaborer un cadre permettant le gel des fonds ou des avoirs financiers et la reconnaissance mutuelle de l'obtention des preuves en matière pénale.

10. La «réaction» couvre la capacité de gérer les effets d'un attentat terroriste et comprend l'aide aux victimes du terrorisme.

11. Tous ces domaines d'action sont étroitement liés à des initiatives sur lesquelles le CEPD s'est déjà prononcé: le programme de Stockholm, les mesures restrictives et le gel des avoirs, la conservation des données, les scanners corporels, les précurseurs d'armes, la biométrie, la décision de Prüm, les dossiers passagers (données PNR), l'accord sur le TFTP (programme de surveillance du financement du terrorisme), le système d'information Schengen, le système d'information sur les visas, la gestion intégrée des frontières, la stratégie de gestion de l'information de l'UE et l'échange transfrontalier de preuves.

12. Les domaines de la «prévention» et de la «protection» sont les plus délicats du point de vue de la protection des données, et ce pour plusieurs raisons.

13. Premièrement, ces domaines reposent par définition sur des analyses de risque prospectives, lesquelles débouchent dans la plupart des cas sur le traitement global et «préventif» de vastes quantités d'informations personnelles concernant des citoyens non suspects (comme, par exemple, le filtrage de l'internet, les frontières électroniques et les scanners de sûreté).

14. Deuxièmement, la communication envisage le renforcement des partenariats entre les autorités répressives et des sociétés privées (telles que les fournisseurs d'accès à l'internet, les établissements financiers et les compagnies de transport) dans l'optique d'un échange d'informations pertinentes et parfois dans le but de leur «déléguer» certaines parties des activités de répression. Cela implique une utilisation accrue par les pouvoirs publics, à des fins répressives, des données à caractère personnel collectées par les sociétés privées à des fins commerciales.

15. Nombre de ces initiatives ont été prises, souvent en réaction rapide à des incidents terroristes, sans un examen approfondi des éventuels doubles emplois ou chevauchements avec des mesures déjà existantes. Dans certains cas, même plusieurs années après leur entrée en vigueur, on ignore encore dans quelle mesure l'intrusion dans la vie privée des citoyens qui a résulté de ces mesures était réellement nécessaire dans tous les cas.

16. Par ailleurs, l'utilisation «préventive» des données à caractère personnel présente plus de risques de déboucher sur de la discrimination. L'analyse préventive des informations suppose la collecte et le traitement de données à caractère personnel concernant de vastes catégories de personnes physiques (par exemple l'ensemble des passagers ou l'ensemble des utilisateurs de l'internet), que celles-ci fassent l'objet ou non de soupçons spécifiques. L'analyse de ces données — en particulier lorsqu'elle est associée à des techniques d'exploration de données — peut avoir pour conséquence que des innocents soient considérés comme suspects uniquement parce que leur profil (âge, sexe, religion, etc.) ou leur mode de vie (par exemple lors de leurs déplacements ou de l'utilisation qu'ils font de l'internet, etc.) correspondent à ceux d'individus liés à des activités terroristes ou soupçonnés d'y être liés. Par conséquent, en particulier dans ce contexte, l'utilisation illégale ou incorrecte d'informations personnelles (parfois sensibles), associée à de vastes pouvoirs coercitifs des autorités répressives, peut déboucher sur une discrimination vis-à-vis de personnes ou de groupes de personnes spécifiques ainsi que sur leur stigmatisation.

17. Dans cette optique, garantir un niveau élevé de protection des données à caractère personnel est également un moyen de lutter contre le racisme, la xénophobie et la discrimination, ce qui, selon la communication, «peu[t] également contribuer à prévenir la radicalisation et le recrutement de terroristes».

2. **Une approche cohérente fondée sur le principe de nécessité**

18. Une remarque générale importante concerne la nécessité de garantir la cohérence ainsi que des rapports clairs entre toutes les communications et initiatives adoptées dans le domaine des affaires intérieures, et en particulier dans celui de la sécurité intérieure. Par exemple, bien que la stratégie européenne de lutte contre le terrorisme soit étroitement liée à la stratégie de gestion de l'information, à la stratégie visant à garantir le respect de la Charte des droits fondamentaux et au modèle européen d'échange d'informations, les rapports entre tous ces documents ne sont pas

([1]) 2002/475/JAI, (JO L 164 du 22.6.2002, p. 3).
([2]) 2008/919/JAI, (JO L 330 du 9.12.2008, p. 21).
([3]) Également annoncé dans le «plan d'action mettant en œuvre le programme de Stockholm» de la Commission [COM(2010) 171 final du 20 avril 2010].

mentionnés de façon explicite et complète. C'est devenu encore plus évident avec l'adoption le 22 novembre 2010 de «La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre» ([1]).

19. Le CEPD recommande dès lors aux institutions de l'UE de veiller à ce que les politiques et initiatives adoptées dans le domaine des affaires intérieures et de la sécurité intérieure soient conçues et appliquées de manière cohérente ainsi que de veiller à établir clairement les relations entre elles, dans le but de permettre des synergies adéquates et positives et d'éviter la duplication des activités et des efforts.

20. Le CEPD recommande en outre que chaque proposition dans ce domaine tienne expressément compte du principe de nécessité. Il conviendrait à cet effet d'évaluer les éventuels chevauchements avec les instruments déjà existants et de limiter la collecte et l'échange des données à caractère personnel à ce qui est vraiment nécessaire pour atteindre les objectifs poursuivis.

21. Par exemple, dans le cas de l'accord avec les États-Unis portant sur le programme de surveillance du financement du terrorisme (TFTP II), le CEPD s'est interrogé sur la mesure dans laquelle cet accord était réellement nécessaire pour obtenir des résultats qui pourraient être obtenus au moyen d'instruments moins intrusifs pour la vie privée, tels que ceux qui sont déjà prévus par le cadre européen et international existant ([2]). Dans le même avis, le CEPD a mis en doute la nécessité de transférer en masse des données à caractère personnel, plutôt que de recourir à une méthode plus ciblée.

22. La communication mentionne parmi les défis qu'il y aura lieu de «s'assurer que ces instruments couvrent les besoins réels (des activités répressives) tout en garantissant le respect intégral du droit à la vie privée et des règles relatives à la protection des données». Le CEPD se félicite de cette reconnaissance explicite et appelle les institutions de l'UE à évaluer attentivement la mesure dans laquelle les instruments déjà existants ainsi que les instruments envisagés couvrent les besoins réels des activités répressives, tout en évitant les chevauchements entre plusieurs mesures ou les restrictions de la vie privée qui ne s'avèrent pas nécessaires. Dans cette optique, les instruments existants devraient faire l'objet de réexamens périodiques visant à déterminer s'ils constituent des moyens efficaces de lutte contre le terrorisme.

23. Dans nombre de ses avis et observations, et en particulier dans son récent avis sur la communication intitulée «Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice» ([3]), le CEPD a recommandé d'évaluer tous les instruments existants en matière d'échange d'informations avant d'en proposer de nouveaux. En effet, l'évaluation de l'efficacité des mesures existantes associée à l'analyse des incidences des nouvelles mesures envisagées sur la vie privée est indispensable et devrait revêtir une importance majeure dans l'action de l'Union européenne dans ce domaine, conformément à l'approche proposée dans le programme de Stockholm.

24. Les chevauchements et les manques d'efficacité devraient donner lieu à des ajustements des choix stratégiques, voire à la consolidation ou à l'abandon des systèmes existants de collecte et de traitement des données.

25. Le CEPD recommande de prêter une attention particulière aux propositions qui débouchent sur une collecte de données à caractère personnel généralisée à l'ensemble des citoyens, plutôt que se limitant aux personnes suspectes. Il convient en outre d'évaluer et de justifier de manière spécifique les cas où le traitement de données à caractère personnel est prévu pour des fins autres que celles auxquelles les données collectées étaient initialement destinées, comme par exemple dans le cas de l'accès à des fins répressives aux données personnelles stockées dans le système Eurodac.

26. La communication souligne qu'un autre défi à venir sera de garantir une politique efficace dans le domaine de la recherche en matière de sécurité, laquelle contribuera à une sécurité de haut niveau. Le CEPD partage le point de vue selon lequel une recherche efficace en matière de sécurité devrait resserrer les liens entre les différents acteurs. Dans cette optique, il est indispensable d'introduire à un stade précoce l'expertise dans le domaine de la protection des données dans la recherche en matière de sécurité, de manière à orienter les options stratégiques et à garantir que la vie privée est pleinement intégrée dans les nouvelles technologies axées sur la sécurité, selon le principe «privacy by design» (prise en compte du respect de la vie privée dès la conception).

3. **En ce qui concerne l'utilisation des mesures restrictives (gel des avoirs)**

27. En ce qui concerne l'utilisation des mesures restrictives (gel des avoirs) à l'égard de pays spécifiques et des terroristes présumés, la jurisprudence de la Cour de justice a confirmé à plusieurs reprises et de façon cohérente que le respect des droits fondamentaux dans la lutte contre le terrorisme est indispensable, et ce dans le but de garantir le respect des droits des citoyens comme la légalité des mesures prises.

28. Le CEPD a déjà contribué par des avis et observations dans ce domaine ([4]), d'un côté en soulignant les améliorations apportées aux procédures mais de l'autre en demandant des améliorations supplémentaires, en particulier s'agissant du droit d'information et d'accès aux données personnelles,

([1]) Voir point 4 du présent avis.
([2]) Avis du CEPD du 22 juin 2010.
([3]) Avis du CEPD du 30 septembre 2010.

([4]) Avis du 28 juillet 2009 sur la proposition de règlement du Conseil modifiant le règlement (CE) n° 881/2002 instituant certaines mesures restrictives spécifiques à l'encontre de certaines personnes et entités liées à Oussama ben Laden, au réseau Al-Qaida et aux Taliban, (JO C 276 du 17.11.2009, p. 1). Avis du 16 décembre 2009 sur différentes propositions législatives instituant certaines mesures restrictives spécifiques à l'encontre de la Somalie, du Zimbabwe, de la Corée du Nord et de la Guinée, (JO C 73 du 23.3.2010, p. 1). Voir également la lettre du CEPD du 20 juillet 2010 concernant trois propositions législatives instituant certaines mesures restrictives a) à l'encontre de M. Milosevic et des personnes de son entourage, b) à l'appui du mandat du Tribunal pénal international pour l'ex-Yougoslavie et c) à l'encontre de l'Érythrée. L'ensemble des avis et observations du CEPD sont disponibles sur son site web: http://www.edps.europa.eu

de la définition claire des restrictions de ces droits et de la disponibilité de recours en justice efficaces et d'un contrôle indépendant.

29. La nécessité d'apporter des améliorations supplémentaires à la procédure et aux garanties disponibles aux personnes inscrites sur une liste a récemment été confirmée par le Tribunal dans l'affaire «Kadi II» ([1]). En particulier, le Tribunal a mis en évidence la nécessité d'informer de manière détaillée la personne inscrite sur une liste des raisons qui ont motivé son inclusion dans ladite liste. Cela se rapproche très fortement des droits, garantis par la législation relative à la protection des données, en vertu desquels toute personne a le droit d'accéder aux données à caractère personnel la concernant et d'en obtenir la rectification, en particulier lorsque ces données sont incorrectes ou obsolètes. Ces droits, expressément mentionnés à l'article 8 de la Charte des droits fondamentaux, constituent les éléments de base de la protection des données et ne peuvent faire l'objet de restrictions que dans la mesure où ces restrictions sont nécessaires, prévisibles et prévues par la loi.

30. Dans cette perspective, le CEPD marque son accord avec la communication concernant le fait que l'un des défis à venir dans le domaine de la politique antiterroriste sera l'utilisation de l'article 75 du TFUE. Cette nouvelle base juridique, introduite par le traité de Lisbonne, permet spécifiquement de prendre des mesures telles que le gel des avoirs à l'encontre de personnes physiques ou morales. Le CEPD recommande d'utiliser cette base juridique également pour établir un cadre de gel des avoirs qui respecte intégralement les droits fondamentaux. Le CEPD se tient à disposition pour contribuer ultérieurement à l'élaboration des instruments et procédures législatives nécessaires, et attend avec impatience d'être consulté de manière adéquate et en temps utile lorsque la Commission — en vertu de son programme de travail pour 2011 — élaborera un règlement spécifique en la matière ([2]).

31. Dans une perspective plus large, il est nécessaire de mettre en place un cadre de protection des données applicable également dans le domaine de la politique étrangère et de sécurité commune. En effet, l'article 16 du TFUE apporte une base juridique pour l'établissement de règles relatives à la protection des données également dans ce domaine. La base juridique et la procédure différentes établies par l'article 39 du traité UE ne s'appliqueront que lorsque des données à caractère personnel sont traitées dans ce domaine par les États membres. Toutefois, même si le traité de Lisbonne appelle à mettre en place ces règles relatives à la protection des données et fournit les instruments nécessaires à cette fin, aucune initiative n'est prévue pour le moment dans la récente communication intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne» ([3]). Dans ce contexte, le CEPD prie instamment la Commission de présenter une proposition portant sur la création d'un cadre de protection des données dans le domaine de la politique étrangère et de sécurité commune.

4. **Respect des droits fondamentaux et coopération internationale**

32. Le chapitre consacré au respect des droits fondamentaux souligne que l'UE se doit d'être exemplaire en ce qui concerne le respect de la Charte des droits fondamentaux, qui doit demeurer le point de référence de toutes ses politiques. Le CEPD se félicite de ce point de vue.

33. Le CEPD approuve également la déclaration selon laquelle le respect des droits fondamentaux est non seulement une exigence juridique, mais aussi une condition essentielle pour promouvoir la confiance mutuelle entre les autorités nationales et obtenir la confiance du grand public.

34. Dans ce contexte, le CEPD recommande de suivre une démarche proactive et de mener des actions concrètes à cette fin, ce qui permettra une mise en œuvre effective de la Charte des droits fondamentaux de l'Union européenne ([4]).

35. Il y aurait lieu de garantir des analyses d'impact sur la vie privée et des consultations précoces des autorités compétentes en matière de protection des données pour l'ensemble des initiatives qui ont des répercussions sur la protection des données à caractère personnel, indépendamment de l'institution qui propose ces initiatives et du domaine concerné.

36. Dans son chapitre consacré à la coopération internationale, la communication souligne par ailleurs la nécessité de créer «les conditions juridiques et politiques nécessaires au renforcement de la coopération avec les partenaires extérieurs de l'UE dans le domaine de la lutte contre le terrorisme».

37. À cet égard, le CEPD rappelle la nécessité d'assurer des garanties adéquates lorsque les données à caractère personnel sont échangées avec les pays tiers et les organisations internationales, afin de garantir que les droits des citoyens dans le domaine de la protection des données sont également respectés de manière appropriée dans le contexte de la coopération internationale.

38. Dans ce contexte, il est également nécessaire de promouvoir la protection des données en coopération avec les pays tiers et les organisations internationales, afin de garantir le respect des normes de l'UE. Cela est en outre conforme à l'intention de la Commission d'élaborer des normes juridiques et techniques élevées en matière de protection des données dans les pays tiers et au niveau international, et de renforcer la coopération avec les pays tiers ([5]).

([1]) Arrêt du 30 septembre 2010 dans l'affaire T-85/09, *Kadi/Commission*; voir en particulier les points 157 et 177.

([2]) Le programme de travail de la Commission pour 2011 [COM(2010) 623 du 27 octobre 2010] mentionne dans son annexe II (Liste indicative des éventuelles initiatives envisagées) un «règlement portant création d'une procédure de gel des fonds des personnes soupçonnées de mener des activités terroristes à l'intérieur de l'UE».

([3]) Communication de la Commission (2010) 609 du 4 novembre 2010.

([4]) Voir communication de la Commission (2010) 573 du 19 octobre 2010 intitulée «Stratégie pour la mise en œuvre effective de la Charte des droits fondamentaux par l'Union européenne».

([5]) Voir communication (2010) 609 intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», pages 16 et 17.

39. Un domaine potentiel évident pour l'action de l'Union européenne dans ce domaine concerne les mesures restrictives (gel des avoirs), dans le contexte desquelles une intense coopération avec les pays tiers et les Nations unies ne devrait pas réduire le niveau élevé de protection des droits fondamentaux garanti par le système juridique de l'UE.

III. **CONCLUSIONS**

40. Le CEPD se félicite de l'attention portée dans la communication aux droits fondamentaux et à la protection des données et recommande des améliorations concrètes supplémentaires dans le domaine de la politique antiterroriste.

41. Le CEPD recommande d'adopter des initiatives concrètes à l'appui du respect des droits fondamentaux dans ce domaine, et notamment du droit à la protection des données à caractère personnel, qui constitue un appui nécessaire pour promouvoir la sécurité juridique, la confiance et la coopération dans la lutte contre le terrorisme, mais qui constitue également une condition juridique indispensable pour l'élaboration des systèmes envisagés.

42. Le CEPD partage également le point de vue selon lequel une approche systématique dans le domaine doit être préférée à une prise de décision axée sur les incidents, en particulier lorsque ces derniers conduisent à la création de nouveaux systèmes de stockage, de collecte et d'échange de données sans une évaluation appropriée des solutions existantes.

43. Le CEPD recommande dès lors aux institutions de l'UE de veiller à ce que les politiques et initiatives adoptées dans le domaine des affaires intérieures et de la sécurité intérieure soient conçues et appliquées de manière cohérente ainsi que de veiller à établir clairement les relations entre elles, dans le but de permettre des synergies adéquates et positives et d'éviter la duplication des activités et des efforts.

44. Dans ce contexte, le CEPD recommande au législateur de l'UE d'intensifier le rôle de la protection des données, en s'engageant à mener des actions spécifiques (dans le respect de délais spécifiques), notamment:

— l'évaluation de l'efficacité des mesures existantes associée à l'analyse de leurs incidences sur la vie privée est indispensable et devrait revêtir une importance majeure dans l'action de l'Union européenne dans ce domaine;

— lorsque de nouvelles mesures sont envisagées, il conviendrait d'évaluer les éventuels chevauchements avec les instruments existants, en tenant compte de leur efficacité, et de limiter la collecte et l'échange des données à caractère personnel à ce qui est vraiment nécessaire pour atteindre les objectifs poursuivis;

— il est nécessaire de proposer un cadre de protection des données applicable également dans le domaine de la politique étrangère et de sécurité commune;

— il y a lieu de proposer une approche complète et globale pour garantir, dans le domaine des mesures restrictives (gel des avoirs), tant l'efficacité des activités répressives que le respect des droits fondamentaux, sur la base de l'article 75 du TFUE;

— la protection des données doit être placée au cœur du débat sur les mesures à prendre dans ce domaine, en garantissant par exemple que des analyses d'impact sur la vie privée et la protection des données sont effectuées et que les autorités compétentes en matière de protection des données sont consultées en temps utile lorsque des propositions sont avancées dans ce domaine;

— il est indispensable d'introduire à un stade précoce l'expertise dans le domaine de la protection des données dans la recherche en matière de sécurité, de manière à orienter les options stratégiques et à garantir que la vie privée est pleinement intégrée dans les nouvelles technologies axées sur la sécurité;

— il est nécessaire de prévoir des garanties adéquates lorsque les données à caractère personnel sont traitées dans le contexte de la coopération internationale, tout en promouvant l'élaboration et l'application de principes en matière de protection des données par les pays tiers et les organisations internationales.

Fait à Bruxelles, le 24 novembre 2010.

Peter HUSTINX

Contrôleur européen de la protection des données