I

(Résolutions, recommandations et avis)

AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du contrôleur européen de la protection des données concernant le rapport final du Groupe de contact à haut niveau UE/États-Unis sur le partage d'informations et la protection de la vie privée et des données à caractère personnel

(2009/C 128/01)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité instituant la Communauté européenne, et notamment son article 286,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment son article 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,

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, et notamment son article 41,

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION — CONTEXTE DE L'AVIS

1. Le 28 mai 2008, la présidence du Conseil de l'Union européenne a annoncé au Coreper, dans la perspective du sommet UE-États-Unis du 12 juin 2008, que le Groupe de contact à haut niveau UE/États-Unis (EU-US High Level Contact Group — ci-après dénommé «HLCG») sur le partage d'informations et la protection de la vie privée et des données à caractère personnel avait établi la version définitive de son rapport. Celui-ci a été publié le 26 juin 2008 ([1]).

2. Ce rapport vise à dégager des principes communs pour la protection de la vie privée et des données à caractère personnel, première étape vers l'échange d'informations avec les États-Unis aux fins de la lutte contre le terrorisme et les formes graves de criminalité transnationale.

3. Dans son annonce, la présidence du Conseil déclare que toutes les idées concernant les actions à mener dans le prolongement de ce rapport seraient les bienvenues, et en particulier les réactions aux recommandations figurant dans le rapport concernant les voies à suivre. Le CEPD répond à cette invitation en formulant le présent avis, sur la base de l'état des lieux tel qu'il a été publié et sans préjudice de toute autre position qu'il pourrait adopter ultérieurement en fonction de l'évolution de la question.

4. Le CEPD note que les travaux du HLCG ont eu pour toile de fond le développement, particulièrement marqué depuis le 11 septembre 2001, des échanges de données entre les États-Unis et l'UE, dans le cadre d'accords internationaux et d'autres types d'instruments. On peut notamment citer les accords conclus par Europol et Eurojust avec les États-Unis, ainsi que les accords PNR et l'affaire Swift, qui ont donné lieu à un échange de lettres entre les responsables européens et américains en vue d'établir des garanties minimales pour la protection des données ([2]).

([1]) Doc. 9831/08, disponible à l'adresse suivante: http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

([2]) — Accord entre les États-Unis d'Amérique et l'Office européen de police (Europol) du 6 décembre 2001, et accord complémentaire entre les États-Unis d'Amérique et Europol relatif à l'échange de données à caractère personnel et d'informations y afférentes, publiés sur le site web d'Europol;
— accord entre les États-Unis d'Amérique et Eurojust du 6 novembre 2006 sur la coopération judiciaire, publié sur le site web d'Eurojust;
— accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007), signé à Bruxelles le 23 juillet 2007 et à Washington le 26 juillet 2007, JO L 204 du 4.8.2007, p. 18;
— échange de lettres entre les autorités des États-Unis et celles de l'UE sur le programme de surveillance du financement du terrorisme («Terrorist Finance Tracking Program»), 28 juin 2007.

5. Par ailleurs, l'UE négocie et adopte également des instruments similaires relatifs à l'échange de données à caractère personnel avec d'autres pays tiers. L'accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) provenant de l'Union européenne par les transporteurs aériens au service des douanes australien en est un exemple récent ([3]).

6. Il ressort de ce contexte que les demandes d'informations à caractère personnel émanant d'autorités répressives de pays tiers ne cessent de s'élargir, et qu'elles ne portent plus uniquement sur les bases de données gouvernementales traditionnelles mais s'étendent aussi à d'autres types de dossiers, notamment des dossiers contenant des données collectées par le secteur privé.

7. Le CEPD juge également important de rappeler, pour éclairer la toile de fond, que la question du transfert de données à caractère personnel à des pays tiers dans le cadre de la coopération policière et judiciaire en matière pénale fait l'objet de la décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale ([4]), qui devrait être adoptée avant la fin de 2008.

8. Il faut s'attendre à ce que cet échange transatlantique d'informations se développe et touche de nouveaux secteurs dans lesquels ont lieu des traitements de données à caractère personnel. Dans ce contexte, un dialogue sur la «répression transatlantique» est tout à la fois opportun et délicat. Il est opportun parce qu'il pourrait fournir un cadre plus clair pour les échanges de données qui ont ou auront lieu. Il est en même temps délicat parce qu'un tel cadre pourrait légitimer des transferts de données massifs dans un domaine — la répression — où les conséquences pour les personnes sont particulièrement graves et où des garanties strictes et fiables sont, de ce fait, d'autant plus nécessaires ([5]).

9. Dans le prochain chapitre du présent avis, le CEPD examinera la situation actuelle et les pistes envisageables. Le chapitre III sera consacré au champ d'application et à la nature d'un instrument qui permettrait le partage d'informations. Au chapitre IV, le CEPD analysera d'un point de vue général les questions juridiques liées au contenu d'un éventuel accord. Il abordera notamment les conditions d'évaluation du niveau de protection offert aux État-Unis et se penchera sur la question de l'utilisation du cadre réglementaire de l'UE comme point de comparaison pour évaluer ce niveau. Ce chapitre contiendra également une liste des exigences de base qu'un tel accord devrait comporter. Enfin, au chapitre V, le CEPD analysera les principes relatifs au respect de la vie privée annexés au rapport du HLCG.

([3]) JO L 213 du 8.8.2008, p. 49.

([4]) Décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, version du 24 juin 2008, disponible à l'adresse suivante: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=fr&DosId=193371

([5]) En ce qui concerne la nécessité d'un cadre juridique clair, voir les chapitres III et IV du présent avis.

II. SITUATION ACTUELLE ET PISTES ENVISAGEABLES

10. Le CEPD estime que la situation actuelle est la suivante: des progrès ont été réalisés en matière de définition de normes communes relatives au partage d'informations et à la protection de la vie privée et des données à caractère personnel.

11. Cependant, les travaux préparatoires nécessaires à tout type d'accord entre l'UE et les États-Unis ne sont pas encore terminés. Des travaux supplémentaires sont nécessaires. Le rapport du HLCG mentionne lui-même un certain nombre de questions en suspens, dont la plus saillante est celle du recours. Un désaccord subsiste quant au champ d'application que doit avoir la protection juridictionnelle ([6]). Cinq autres questions en suspens sont recensées au chapitre 3 du rapport. En outre, comme on le montrera dans le présent avis, de nombreuses autres questions ne sont pas encore réglées, telles que le champ d'application et la nature d'un instrument relatif au partage d'informations.

12. Le fait que l'option privilégiée dans le rapport soit un accord contraignant — le CEPD partageant cette préférence — doit inciter à la plus grande prudence. Des préparatifs supplémentaires rigoureux et approfondis sont nécessaires avant qu'un accord puisse être conclu.

13. Enfin, le CEPD estime que la meilleure solution serait de conclure un accord dans le cadre du traité de Lisbonne, pour autant, naturellement, que celui-ci entre en vigueur. On éviterait ainsi toute insécurité juridique quant à la séparation entre les piliers de l'UE. En outre, la pleine participation du Parlement européen serait garantie, ainsi que le contrôle juridictionnel de la Cour de justice.

14. Dans ces circonstances, l'établissement d'une feuille de route en vue d'un éventuel accord ultérieur constituerait la meilleure solution. Cette feuille de route pourrait prévoir les éléments suivants:

— des orientations pour la poursuite des travaux du HLCG (ou de tout autre groupe), accompagnées d'un calendrier;

— à un stade précoce, un débat et, éventuellement, un accord sur des questions fondamentales telles que le champ d'application et la nature de l'accord;

— sur la base d'une vision commune de ces questions fondamentales, l'élaboration de principes relatifs à la protection des données;

— la participation des parties intéressées à différentes étapes de la procédure;

— pour ce qui concerne la partie européenne, la prise en compte des contraintes institutionnelles.

([6]) Page 5 du rapport, point C.

III. **CHAMP D'APPLICATION ET NATURE D'UN INSTRUMENT RELATIF AU PARTAGE D'INFORMATIONS**

15. Le CEPD considère qu'il est indispensable de définir clairement le champ d'application et la nature d'un éventuel instrument édictant des principes relatifs à la protection des données, comme première étape de son élaboration.

16. En ce qui concerne le champ d'application, les questions importantes auxquelles il convient de répondre sont les suivantes:

— Quels sont les acteurs concernés, tant dans le domaine de la répression qu'en-dehors de celui-ci?

— Qu'entend-on par «fins répressives», et quel est leur lien avec d'autres finalités telles que la sécurité nationale et, plus spécifiquement, le contrôle des frontières et la santé publique?

— Comment l'instrument s'inscrirait-il dans le cadre d'un espace transatlantique global de sécurité?

17. Lors de la définition de la nature de l'instrument, il convient de clarifier les points suivants:

— Le cas échéant, dans le cadre de quel pilier l'instrument sera-t-il négocié?

— L'instrument aura-t-il un caractère contraignant pour l'UE et les États-Unis?

— Aura-t-il un effet direct, c'est-à-dire contiendra-t-il pour les particuliers des droits et des obligations dont le respect pourra être imposé par une autorité judiciaire?

— L'instrument autorisera-t-il lui-même l'échange d'informations, ou fixera-t-il, pour cet échange, des normes minimales qui devront être complétées par des accords spécifiques?

— Quel sera le lien entre l'instrument projeté et les instruments existants? Les respectera-t-il, les remplacera-t-il ou les complétera-t-il?

III. 1. **Champ d'application de l'instrument**

Acteurs concernés

18. Bien qu'aucune indication claire ne figure dans le rapport du HLCG quant au champ d'application précis du futur instrument, on peut déduire des principes qui s'y trouvent mentionnés qu'il devrait couvrir tant les transferts entre acteurs privés et publics ([7]) que les transferts entre autorités publiques.

([7]) Voir, en particulier, le chapitre 3 du rapport, intitulé «Outstanding issues pertinent to transatlantic relations» (Questions en suspens se rapportant aux relations transatlantiques), point 1: «Consistency in private entities obligations during data transfers» (Cohérence des obligations des entités privées lors des transferts de données).

— Entre acteurs privés et publics:

19. Le CEPD perçoit la logique de l'applicabilité d'un futur instrument aux transferts entre acteurs privés et publics. L'élaboration d'un tel instrument s'inscrit dans le contexte des demandes d'informations adressées ces dernières années par les États-Unis à des parties privées. Le CEPD constate en effet que les acteurs privés deviennent une source d'informations systématique dans le domaine de la répression, que ce soit au niveau de l'UE ou au niveau international ([8]). L'affaire SWIFT, dans laquelle le transfert systématique et massif de données a été réclamé à une société privée par les autorités répressives d'un État tiers, a constitué un précédent majeur ([9]). La collecte de données PNR auprès des compagnies aériennes s'inscrit dans cette même logique. Dans son avis sur un projet de décision-cadre relative à un système PNR européen, le CEPD s'est déjà interrogé sur la légitimité de cette tendance ([10]).

20. Deux autres motifs incitent à faire preuve de réticence en ce qui concerne l'inclusion des transferts entre acteurs privés et publics dans le champ d'application d'un futur instrument.

21. Premièrement, cette inclusion pourrait avoir un effet non désiré sur le propre territoire de l'UE. Le CEPD craint fortement que l'acceptation du principe selon lequel les données de sociétés privées (comme les institutions financières) peuvent être transférées à des pays tiers n'entraîne une forte pression pour que ce même type de données puisse également être mis à la disposition des autorités répressives au sein de l'UE. Le système PNR est un exemple de cette évolution indésirable: il a débuté par une collecte massive, par les États-Unis, de données relatives aux passagers, pour être ensuite transposé dans le contexte interne européen ([11]), sans que la nécessité et la proportionnalité du système aient été clairement démontrées.

22. Deuxièmement, dans son avis sur la proposition de la Commission concernant un système PNR européen, le CEPD a également soulevé la question du cadre qui, en

([8]) Voir, à ce sujet, l'avis du CEPD du 20 décembre 2007 sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives, JO C 110 du 1.5.2008, p. 1. «Jusqu'à présent, l'on constatait une séparation claire entre les activités répressives et celles du secteur privé, les missions répressives étant effectuées par des services ad hoc, en particulier les forces de police, et le secteur privé étant sollicité au cas par cas pour communiquer des données à caractère personnel à ces services répressifs. On assiste aujourd'hui à une tendance visant à obliger les acteurs privés à coopérer systématiquement à des fins répressives».

([9]) Voir l'avis 10/2006 du Groupe «Article 29» du22 novembre 2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT), WP 128.

([10]) Avis du 20 décembre 2007, op. cit.

([11]) Voir la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives, mentionné dans la note de bas de page nº 8, en cours d'examen au sein du Conseil.

matière de protection des données (premier ou troisième pilier), doit s'appliquer aux conditions d'une coopération entre acteurs publics et privés: les règles devraient-elles être fondées sur la qualité du responsable du traitement (secteur privé) ou sur la finalité poursuivie (répression)? La frontière entre le premier et le troisième pilier est loin d'être claire lorsque des acteurs privés sont soumis à l'obligation de traiter des données à caractère personnel à des fins répressives. Il est, à cet égard, significatif que l'avocat général BOT, dans ses récentes conclusions sur une affaire relative à la conservation de données [12], propose une ligne de démarcation pour les cas visés ci-dessus, en ajoutant toutefois: «Cette ligne de démarcation n'est certes pas exempte de toute critique et peut paraître, à certains égards, artificielle». Le CEPD note également que l'arrêt de la Cour [13] relatif aux données PNR ne répond pas totalement à la question du cadre juridique applicable. À titre d'exemple, le fait que certaines activités ne soient pas couvertes par la directive 95/46/CE ne signifie pas nécessairement qu'elles peuvent être réglementées dans le cadre du troisième pilier. En conséquence, cet arrêt laisse sans doute subsister un vide juridique en ce qui concerne la législation applicable et, en tout état de cause, crée une insécurité juridique quant aux garanties juridiques dont disposent les personnes concernées.

23. Dans cette optique, le CEPD souligne qu'il convient de veiller à ce qu'un futur instrument contenant des principes généraux relatifs à la protection des données ne puisse légitimer en tant que tel le transfert transatlantique de données à caractère personnel entre des parties privées et publiques. Ce transfert ne peut être prévu dans un futur instrument que si:

— ce dernier précise que le transfert n'est autorisé que lorsqu'il s'avère absolument nécessaire pour une finalité précise, la décision devant être prise au cas par cas;

— le transfert proprement dit est assorti de garanties élevées en matière de protection des données (telles qu'elles sont décrites dans le présent avis).

En outre, le CEPD souligne l'insécurité qui règne quant au cadre juridique applicable en matière de protection des données et recommande dès lors, en tout état de cause, de ne pas prévoir, en l'état l'actuel de la législation de l'UE, le transfert de données à caractère personnel entre parties privées et publiques.

— Entre autorités publiques:

24. La portée exacte de l'échange d'informations est peu claire. La première étape des travaux à mener en vue de l'élaboration d'un instrument commun devrait consister à préciser le champ d'application que l'on envisage de donner à ce dernier. Des questions subsistent notamment en ce qui concerne les points suivants:

— Pour ce qui est des bases de données situées dans l'UE, l'instrument portera-t-il sur les bases de données centralisées gérées (en partie) par l'UE, telles que les bases de données d'Europol et d'Eurojust, sur les bases de données décentralisées gérées par les États membres, ou sur les deux catégories?

— Le champ d'application de l'instrument couvrira-t-il les réseaux interconnectés? Autrement dit, les garanties prévues porteront-elles sur les données échangées entre États membres ou agences, dans l'UE comme aux États-Unis?

— L'instrument couvrira-t-il uniquement les échanges entre bases de données dans le domaine répressif (police, justice et éventuellement, douanes) ou englobera-t-il également d'autres bases de données, telles que les bases de données fiscales?

— L'instrument concernera-t-il aussi les bases de données des agences nationales de sécurité, ou autorisera-t-il l'accès de ces agences aux bases de données des services répressifs situées sur le territoire de l'autre partie contractante (accès des agences de l'UE aux bases de données des États-Unis et vice versa)?

— L'instrument prévoira-t-il un transfert d'informations au cas par cas, ou un accès permanent aux bases de données existantes? Cette dernière hypothèse soulèverait certainement des questions quant à son caractère proportionnel, comme examiné plus en détail au chapitre V, point 3.

Finalité répressive

25. La définition de la finalité d'un accord éventuel est également source d'incertitude. Les finalités répressives sont clairement indiquées dans l'introduction, ainsi que dans le premier principe annexé au rapport, et elles feront l'objet d'une analyse plus approfondie au chapitre IV du présent avis. Le CEPD relève d'ores et déjà qu'il ressort de ces indications que les échanges de données porteront sur les questions relevant du troisième pilier, mais que l'on peut se demander s'il ne s'agit pas uniquement d'une première étape vers un échange plus large d'informations. Il paraît clair que les objectifs de «sécurité publique» cités dans le rapport comprennent la lutte contre le terrorisme, la criminalité organisée et d'autres formes de criminalité. L'instrument est-il toutefois destiné à couvrir également les échanges de données dans d'autres domaines d'intérêt public, tels que la protection de la santé publique?

26. Le CEPD recommande de limiter la finalité à des traitements de données définis avec précision et de justifier les choix stratégiques qui sont à l'origine de cette définition.

[12] Conclusions de l'avocat général BOT du 14 octobre 2008 dans l'affaire C-301/06, Irlande/Parlement et Conseil, point 108.

[13] Arrêt de la Cour du 30 mai 2006 dans les affaires jointes C-317/04 et C-318/04, Parlement européen/Conseil (C-317/04) et Commission des Communautés européennes (C-318/04), Recueil 2006, p. I-4721.

Un espace transatlantique global de sécurité

27. La portée très large du rapport doit être replacée dans le contexte de l'espace transatlantique global de sécurité examiné par le «Groupe sur l'avenir de la politique intérieure» ([14]). Dans son rapport publié en juin 2008, ce groupe met l'accent, dans une certaine mesure, sur la dimension extérieure de la politique intérieure. Il estime que «*d'ici 2014, l'Union européenne devra s'interroger sur l'objectif politique de créer une zone de coopération euro-atlantique dans le domaine de la liberté, de la sécurité, et de la justice en partenariat avec les États-Unis*». Cette coopération irait au-delà de la sécurité au sens strict et inclurait, au minimum, les sujet traités au titre IV du traité CE, tels que l'immigration, les visas, l'asile et la coopération en matière civile. Il convient de se demander dans quelle mesure un accord sur les principes fondamentaux relatifs à la protection des données, tels que ceux mentionnés dans le rapport du HLCG, pourrait et devrait constituer la base d'un échange d'informations dans un domaine aussi vaste.

28. En principe, d'ici 2014, la structure en piliers disparaîtra et il n'existera qu'une seule base juridique pour la protection des données dans l'UE (dans le cadre du traité de Lisbonne, article 16 du traité sur le fonctionnement de l'Union européenne). Néanmoins, le fait qu'il existe une harmonisation au niveau de l'UE en ce qui concerne la *réglementation* de la protection des données ne signifie pas que tout accord conclu avec un pays tiers pourrait autoriser le *transfert* de données à caractère personnel, quelle que soit la finalité poursuivie. Selon le contexte et les conditions du traitement, des garanties adaptées en matière de protection des données pourraient être requises dans des domaines spécifiques tels que la répression. Le CEPD recommande de tenir compte des conséquences de ces différentes considérations lors de l'élaboration d'un futur accord.

III.2. **Nature de l'accord**

Cadre institutionnel européen

29. Pour le court terme en tout état de cause, il est essentiel de déterminer le pilier au titre duquel l'accord sera négocié, notamment afin de savoir quel sera le cadre réglementaire interne en matière de protection des données sur lequel cet accord aura des incidences. S'agira-t-il du cadre en vigueur au titre du premier pilier — principalement la directive 95/46/CE et son régime spécifique pour le transfert de données aux pays tiers — ou de celui relevant du troisième pilier, qui prévoit un régime moins strict pour ce type de transfert? ([15])

30. Si les objectifs répressifs sont prédominants, comme indiqué précédemment, le rapport du HLCG mentionne cependant la collecte de données auprès d'acteurs privés; les finalités peuvent également être interprétées de façon large et aller au-delà de la sécurité proprement dite, pour toucher à des questions liées à l'immigration et au contrôle des frontières, mais aussi éventuellement à la santé publique. Compte tenu de ces incertitudes, il serait hautement préférable d'attendre l'harmonisation des piliers dans le cadre du droit européen, comme le prévoit le traité de Lisbonne, afin d'établir clairement la base juridique des négociations et le rôle précis des institutions européennes, en particulier le Parlement européen et la Commission.

Caractère contraignant de l'instrument

31. Il conviendrait de préciser si les conclusions des discussions déboucheront sur un mémorandum d'accord ou un autre instrument non contraignant, ou si elles conduiront à un accord international contraignant.

32. Le CEPD partage la préférence, manifestée dans le rapport, pour un accord contraignant. Un accord officiel contraignant est, selon lui, une condition préalable indispensable à tout transfert de données à l'extérieur de l'UE, quelle que soit sa finalité. Aucun transfert de données ne peut avoir lieu vers un pays tiers sans conditions et garanties adéquates fixées dans un cadre juridique spécifique (et contraignant). En d'autres termes, un mémorandum d'accord ou un autre instrument non contraignant peut être utile pour fournir des orientations en vue de la négociation d'accords contraignants ultérieurs, mais ne permettra pas de faire l'économie d'un accord contraignant.

Effet direct

33. Les dispositions de l'instrument devraient être contraignantes tant pour les États-Unis que pour l'UE et ses États membres.

34. Il conviendrait également de veiller à ce que les particuliers puissent exercer leurs droits, et notamment celui de former un recours, sur la base des principes fixés. Selon le CEPD, le meilleur moyen d'y parvenir est de formuler les dispositions de fond de l'instrument de manière à ce qu'elles aient un effet direct pour les résidents de l'Union européenne et qu'elles puissent être invoquées devant un tribunal. L'effet direct des dispositions de l'accord international, ainsi que les conditions de sa transposition en droit interne européen et national afin de garantir l'effectivité des mesures, doivent dès lors être indiqués clairement dans l'instrument.

Relation avec d'autres instruments

35. Il est également fondamental de se poser la question de savoir dans quelle mesure l'accord est autonome ou doit être complété au cas par cas par d'autres accords portant sur des échanges spécifiques de données. Il est en effet peu probable qu'un seul accord puisse couvrir de manière

([14]) Rapport du groupe consultatif informel de haut niveau sur l'avenir de la politique intérieure européenne, «Liberté, sécurité, protection de la vie privée — Les affaires intérieures européennes dans un monde ouvert», juin 2008, disponible sur register.consilium.europa.eu

([15]) Voir les articles 11 et 13 de la décision-cadre relative à la protection des données à caractère personnel, citée au point 7 du présent avis.

adéquate, par une seule série de normes, les spécificités multiples du traitement de données dans le cadre du troisième pilier. On peut encore davantage douter qu'un seul accord puisse *permettre*, sans discussions ou garanties supplémentaires, l'approbation inconditionnelle de tout transfert de données à caractère personnel, quelles que soient la finalité du transfert et la nature des données concernés. En outre, les accords conclus avec des pays tiers ne sont pas nécessairement permanents, car ils peuvent être liés à des menaces particulières, faire l'objet d'un réexamen ou être assortis de clauses de limitation dans le temps. Par ailleurs, des normes minimales communes reconnues dans un instrument contraignant pourraient faciliter toute discussion ultérieure sur le transfert de données à caractère personnel en rapport avec une base de données ou des traitements spécifiques.

36. Le CEPD préconise donc, plutôt qu'un accord autonome, l'élaboration d'une série minimale de critères applicables à la protection des données, qui devraient être complétés au cas par cas par des dispositions spécifiques, comme indiqué dans le rapport du HLCG. Ces dispositions spécifiques complémentaires constitueraient une condition préalable à l'autorisation de tout transfert de données dans chaque cas particulier. On favoriserait ainsi une approche harmonisée en matière de protection des données.

Application aux instruments existants

37. Il conviendrait aussi d'examiner comment un éventuel accord général s'articulerait avec les accords déjà existants conclus entre l'UE et les États-Unis. Il est à noter que ces accords existants ne possèdent pas le même caractère contraignant: c'est le cas, notamment, de l'accord PNR (celui qui présente la plus grande sécurité juridique), des accords Europol et Eurojust, ou de l'échange de lettres dans l'affaire SWIFT ([16]). Un nouveau cadre général viendrait-il compléter ces instruments, ou ceux-ci resteraient-ils inchangés, le nouveau cadre ne s'appliquant qu'aux futurs échanges de données à caractère personnel? Le CEPD considère que, pour garantir la cohérence juridique, il serait approprié de fixer une série harmonisée de règles, qui s'appliqueraient à la fois aux accords contraignants existants et futurs sur les transferts de données et les compléteraient.

38. L'application de l'accord général aux instruments existants présenterait l'avantage de renforcer le caractère contraignant de ces derniers, ce qui serait particulièrement opportun dans le cas des instruments qui ne sont pas juridiquement contraignants, comme l'échange de lettres dans l'affaire SWIFT, car cela imposerait l'observation d'une série de principes généraux en matière de respect de la vie privée.

IV. ÉVALUATION JURIDIQUE GÉNÉRALE

39. Dans le présent chapitre, on examinera la méthode à suivre pour évaluer le niveau de protection d'un cadre ou d'un instrument spécifique, et on abordera notamment la question des points de comparaison à utiliser et des exigences de base nécessaires.

([16]) Voir la note de bas de page n° 2.

Niveau de protection adéquat

40. Selon le CEPD, il devrait être clair qu'un des principaux résultats d'un futur instrument sera que le transfert de données à caractère personnel vers les États-Unis ne pourra avoir lieu que si les autorités de ce pays garantissent un niveau de protection adéquat (et vice versa).

41. Le CEPD considère qu'il ne peut exister de garanties suffisantes quant au niveau de protection des données à caractère personnel que si une véritable analyse du caractère adéquat de ce niveau de protection est mise en place. Il estime que, soumis à une telle analyse, un accord-cadre général d'une portée aussi vaste que celle envisagée dans le rapport du HLCG obtiendrait difficilement, en tant que tel, des résultats satisfaisants. L'adéquation du niveau de protection offert par l'accord général ne pourra être reconnue que si celui-ci est complété par des accords spécifiques conclus au cas par cas et offrant également un niveau de protection suffisant.

42. L'appréciation du niveau de protection offert par des pays tiers n'est pas un exercice inhabituel, en particulier pour la Commission européenne: le caractère adéquat de cette protection est, en vertu du premier pilier, une condition préalable au transfert. Elle a été mesurée à plusieurs occasions au titre de l'article 25 de la directive 95/46/CE sur la base de critères spécifiques, et confirmée par des décisions de la Commission européenne ([17]). Dans le cadre du troisième pilier, aucun système similaire n'est explicitement prévu: la vérification du caractère adéquat du niveau de protection n'est prescrite que dans le cas spécifique prévu aux articles 11 et 13 de la décision-cadre sur la protection des données ([18]) — qui n'a pas encore été adoptée — et relève de la responsabilité des États membres.

43. En l'espèce, l'exercice porte sur des finalités répressives, et les discussions sont menées par la Commission, sous la supervision du Conseil. Le contexte est différent de celui dans lequel a été réalisée l'évaluation des principes de la «sphère de sécurité» ou de l'adéquation de la législation canadienne, et se rapproche plutôt de celui dans lequel ont eu lieu les récentes négociations PNR avec les États-Unis et l'Australie, menées dans un cadre juridique relevant du troisième pilier. Cependant, les principes préconisés par le HLCG ont également été mentionnés dans le cadre du programme d'exemption de visa, qui concerne les frontières et l'immigration et, par conséquent, des questions relevant du premier pilier.

44. Le CEPD recommande que toute analyse de l'adéquation réalisée dans le cadre d'un futur instrument repose sur les expériences acquises dans ces différents domaines. Il préconise le développement, dans le cadre d'un futur instrument

([17]) Les décisions de la Commission constatant l'adéquation du niveau de protection des données à caractère personnel assuré par des pays tiers, notamment l'Argentine, le Canada, la Suisse, les États-Unis, Guernesey, l'Île de Man et Jersey, peuvent être consultées à l'adresse suivante: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_fr.htm

([18]) Ce cas concerne uniquement le transfert par un État membre, vers un pays tiers ou une instance internationale, de données reçues de l'autorité compétente d'un autre État membre.

et sur la base de critères similaires, de la notion d'«adéquation» utilisée dans les analyses menées précédemment.

Reconnaissance mutuelle — réciprocité

45. Le deuxième élément du niveau de protection est lié à la reconnaissance mutuelle des systèmes de l'UE et des États-Unis. Dans son rapport, le HLCG indique, à cet égard, que l'objectif consisterait à «obtenir la reconnaissance, par chacune des parties, de l'efficacité des systèmes de protection de la vie privée et des données de l'autre partie dans les domaines couverts par ces principes» ([19]), et de parvenir à «une application équivalente et réciproque de la législation en matière de protection de la vie privée et des données à caractère personnel» (*traduction du Conseil*).

46. Selon le CEPD, il va de soi que la reconnaissance mutuelle (ou la réciprocité) n'est possible que si un niveau de protection adéquat est garanti. Autrement dit, le futur instrument devrait fixer un niveau minimum harmonisé de protection (par une appréciation du niveau de protection offert, compte tenu de la nécessité de conclure des accords spécifiques au cas par cas). La réciprocité ne pourra être admise qu'à cette condition.

47. Le premier élément à prendre en considération est la réciprocité des dispositions de fond relatives à la protection des données. Selon le CEPD, un accord devrait traiter cette notion d'une manière qui garantisse, d'une part, que les traitements de données effectués sur le territoire de l'UE (et des États-Unis) respectent intégralement les législations internes en matière de protection des données et, d'autre part, que les traitements réalisés à l'extérieur du pays d'origine des données et entrant dans le champ d'application de l'accord respectent les principes relatifs à la protection des données énoncés dans l'accord.

48. Le deuxième élément à prendre en compte est la réciprocité des mécanismes de recours. Il convient de veiller à ce que les citoyens européens disposent de voies de recours adéquates lorsque des données qui les concernent sont traitées aux États-Unis (indépendamment de la législation applicable à ce traitement), mais aussi à ce que l'Union européenne et ses États membres accordent des droits équivalents aux citoyens des États-Unis.

49. Le troisième élément à considérer est la réciprocité de l'accès des autorités répressives aux données à caractère personnel. Si un instrument autorise l'accès des autorités des États-Unis aux données provenant de l'Union européenne, la réciprocité impliquerait que les autorités de l'UE aient, elles aussi, accès aux données provenant des États-Unis. La réciprocité ne doit pas nuire à l'effectivité de la protection des personnes concernées. Ceci constitue une condition préalable à l'octroi aux autorités répressives d'un accès «transatlantique». Concrètement, cela signifie que:

— l'accès direct des autorités des États-Unis aux données se trouvant sur le territoire de l'UE (et vice versa) ne devrait pas être autorisé. L'accès ne devrait être accordé que de manière indirecte, dans le cadre d'un système d'exportation «push»;

— cet accès devrait avoir lieu sous le contrôle des autorités chargées de la protection des données et des autorités judiciaires du pays dans lequel le traitement de données est effectué;

— l'accès des autorités des États-Unis aux bases de données de l'UE devrait se faire dans le respect des dispositions de fond relatives à la protection des données (voir ci-dessus), en offrant aux personnes concernées toutes les voies de recours.

Précision de l'instrument

50. La spécification des conditions d'évaluation (adéquation, équivalence, reconnaissance mutuelle) est essentielle, car elle déterminera le contenu de l'instrument pour ce qui est de la précision, de la sécurité juridique et de l'efficacité de la protection. Le contenu d'un futur instrument doit être précis et fiable.

51. En outre, il devrait être clair que tout accord spécifique conclu ultérieurement devra inclure des garanties détaillées et complètes en matière de protection des données en rapport avec l'objet de l'échange de données envisagé. Seul ce double niveau de principes concrets concernant la protection des données garantira l'étroite complémentarité nécessaire entre l'accord général et les accords spécifiques, comme on l'a déjà indiqué aux points 35 et 36 du présent avis.

Élaboration d'un modèle pour les autres pays tiers

52. La question de savoir dans quelle mesure un accord avec les États-Unis pourrait servir de modèle pour d'autres pays tiers mérite une attention particulière. Le CEPD note que, outre les États-Unis, le rapport du «Groupe sur l'avenir de la politique intérieure» mentionné précédemment cite également la Russie comme partenaire stratégique de l'UE. Pour autant que les principes soient neutres et conformes aux garanties fondamentales de l'UE, ils pourraient constituer un précédent utile. Toutefois, les particularités liées, par exemple, au cadre juridique du pays destinataire ou à la finalité du transfert empêcheront une transposition pure et simple de l'accord. La situation des pays tiers sur le plan de la démocratie sera également déterminante: il conviendra de s'assurer que les principes fixés seront effectivement garantis et respectés dans le pays destinataire.

Quels critères appliquer pour évaluer le niveau de protection?

53. Pour être implicitement ou explicitement adéquat, le niveau de protection doit, en tout état de cause, être conforme au cadre juridique international et européen, et en particulier aux garanties fixées d'un commun accord en matière de

([19]) Point A intitulé «Binding international agreement» (Accord international contraignant), p. 8.

protection des données. Celles-ci sont inscrites dans les principes directeurs des Nations unies, la convention 108 du Conseil de l'Europe et son protocole additionnel, les lignes directrices de l'OCDE et la proposition de décision-cadre relative à la protection des données, ainsi que, pour les aspects relevant du premier pilier, dans la directive 95/46/CE ([20]). Tous ces instruments énoncent des principes similaires, largement reconnus comme constituant les éléments essentiels de la protection des données à caractère personnel.

54. L'impact d'un accord potentiel tel que celui envisagé dans le rapport du HLCG rend d'autant plus importante la prise en considération des principes susmentionnés. Un instrument couvrant l'intégralité du secteur *répressif* d'un pays tiers serait en effet sans précédent. Les décisions existantes en matière d'adéquation dans le cadre du premier pilier et les accords conclus avec des pays tiers dans le cadre du troisième pilier de l'UE (Europol, Eurojust) ont toujours été liés à un transfert de données spécifique, alors que, dans le cas présent, des transferts d'une portée bien plus vaste pourraient devenir possibles, compte tenu de l'ampleur de la finalité poursuivie (lutte contre les infractions pénales, sécurité nationale et publique, contrôles aux frontières) et du nombre — inconnu jusqu'ici — de bases de données concernées.

Exigences de base

55. Les conditions à respecter dans le cadre du transfert de données à caractère personnel vers des pays tiers sont énoncées dans un document de travail du Groupe «Article 29» ([21]). Tout accord sur des principes minimaux en matière de respect de la vie privée devrait être soumis à un examen de conformité destiné à vérifier l'efficacité des garanties relatives à la protection des données.

— Quant au fond: les principes relatifs à la protection des données devraient prévoir un niveau de protection élevé et être conformes aux principes de l'UE. Les douze principes énoncés dans le rapport du HLCG seront analysés plus en profondeur dans cette optique au chapitre V du présent avis.

— En ce qui concerne la spécificité: en fonction de la nature de l'accord, et en particulier s'il s'agit d'un accord international officiel, les règles et procédures devraient être suffisamment détaillées pour permettre une mise en œuvre effective.

— En ce qui concerne la supervision: pour garantir le respect des règles fixées, des mécanismes de contrôle spécifiques devraient être mis en place, tant au niveau interne (audits) qu'au niveau externe (évaluations). Les deux parties à l'accord doivent y avoir accès sur un pied d'égalité. La surveillance requiert des mécanismes permettant de vérifier le respect de l'accord au niveau global, tels que des mécanismes d'évaluation conjointe, et au niveau individuel, tels que le recours personnel.

56. Outre ces trois exigences de base, il convient de prêter une attention particulière aux spécificités liées au traitement de données à caractère personnel dans un contexte répressif. Il s'agit en effet d'un domaine où les droits fondamentaux sont susceptibles de connaître certaines limitations. Des garanties doivent donc être adoptées pour compenser la limitation de ces droits des particuliers, notamment en qui concerne les aspects ci-dessous, eu égard à leur incidence sur les particuliers:

— transparence: l'information et l'accès aux données à caractère personnel peuvent être limités dans un contexte répressif, en raison, par exemple, de la discrétion nécessaire aux enquêtes. Dans l'UE, des mécanismes supplémentaires sont habituellement mis en place pour compenser cette limitation des droits fondamentaux (faisant souvent intervenir des autorités indépendantes chargées de la protection des données); il convient de vérifier qu'il existe des mécanismes de compensation similaires lors du transfert d'informations vers un pays tiers;

— recours: pour les raisons susmentionnées, les particuliers devraient disposer de différentes possibilités pour faire valoir leurs droits, notamment via une autorité de surveillance indépendante et devant un tribunal;

— conservation des données: la justification de la durée de conservation des données pourrait ne pas être transparente. Il convient de prendre des mesures afin que cela n'empêche pas les personnes concernées ou les autorités de contrôle d'exercer effectivement leurs droits;

([20]) — Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, adoptés par l'Assemblée générale le 14 décembre 1990, consultables à l'adresse suivante: http://www.unhchr.ch/french/html/menu3/b/71_fr.htm
— Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981, consultable à l'adresse suivante: http://www.conventions.coe.int/Treaty/FR/Treaties/Html/108.htm
— Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptées le 23 septembre 1980, consultables à l'adresse suivante: http://www.oecd.org/document/53/0,3343,fr_2649_34255_15591797_1_1_1_1,00.html
— Proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, consultable à l'adresse suivante: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=fr&DosId=193371
— 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, JO L 281 du 23.11.1995, p. 31.

([21]) Document de travail du 24 juillet 1998 intitulé «Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données», WP 12.

— obligation, pour les autorités répressives, de rendre des comptes: en l'absence d'une transparence effective, les mécanismes permettant aux acteurs individuels ou institutionnels d'exercer un contrôle ne peuvent qu'avoir une portée limitée. Il n'en demeure pas moins indispensable d'établir fermement ce contrôle, compte tenu du caractère sensible des données et des mesures coercitives qui peuvent être prises contre des particuliers sur la base du traitement de données. L'obligation de rendre des comptes est une question déterminante aux fins du contrôle par le pays destinataire, mais également par le pays ou la région d'où proviennent les données. De tels mécanismes de contrôle sont prévus dans des accords spécifiques, tels que l'accord PNR, et le CEPD recommande vivement d'en prévoir également dans l'instrument général.

V. **ANALYSE DES PRINCIPES**

Introduction

57. Dans le présent chapitre, les douze principes énoncés dans le document du HLCG seront analysés sous l'angle suivant:

— ces principes font ressortir certaines convergences de vues entre les États-Unis et l'UE en ce qui concerne les principes, car on peut relever des similitudes avec ceux figurant dans la convention 108;

— cependant, un accord sur le niveau des principes ne suffit pas. Un instrument juridique devrait être avoir une force suffisante pour garantir leur respect;

— le CEPD déplore que les principes ne soient pas accompagnés d'une note explicative;

— il devrait être clair, avant d'entrer dans la description des principes, que les deux parties partagent la même interprétation des termes utilisés, par exemple en ce qui concerne la notion d'informations à caractère personnel ou de personnes protégées. À cet égard, des définitions seraient opportunes.

1. Spécification de la finalité

58. Selon le premier principe énoncé dans l'annexe du rapport du HLCG, les informations à caractère personnel doivent être traitées à des fins répressives légitimes. Comme indiqué précédemment, il s'agit, pour l'Union européenne, de la prévention, de la détection, de la recherche et de la poursuite des infractions pénales. Les États-Unis, pour leur part, considèrent que les finalités répressives n'englobent pas seulement les infractions pénales mais comprennent également les fins liées aux contrôles aux frontières, à la sécurité publique et à la sécurité nationale. Les conséquences de ces divergences entre les finalités déclarées de l'UE et celles des États-Unis ne sont pas claires. Dans son rapport, le HLCG indique que, dans la pratique, ces finalités peuvent coïncider dans une large mesure, mais il demeure essentiel de savoir exactement dans quelle mesure elles *ne* coïncident *pas*. Dans le domaine de la répression, étant donné l'incidence des mesures prises sur les particuliers, le principe de la limitation des finalités doit être strictement observé et les objectifs déclarés doivent être clairs et bien définis. Compte tenu de la réciprocité envisagée dans le rapport, le rapprochement de ces finalités semble également fondamental. Bref, une clarification de l'interprétation de ce principe s'impose.

2. Intégrité/Qualité des données

59. Le CEPD accueille favorablement la disposition prévoyant que les informations à caractère personnel doivent être exactes, pertinentes, disponibles en temps utile et complètes, ainsi que l'exige la licéité du traitement. Ce principe est une condition fondamentale de tout traitement de données efficace.

3. Nécessité/Proportionnalité

60. Ce principe établit un lien clair entre les informations collectées et la nécessité de disposer de ces informations pour atteindre une fin répressive prévue par la loi. Cette obligation de disposer d'une base légale est un élément positif aux fins de l'établissement de la légitimité du traitement. Le CEPD note néanmoins que, bien que cela renforce la sécurité juridique entourant le traitement, la base légale du traitement est un acte législatif d'un pays tiers. Or, une loi d'un pays tiers ne peut en tant que telle constituer une base légitime pour le transfert de données à caractère personnel ([22]). Dans son rapport, le HLCG semble considérer que la légitimité de la loi d'un pays tiers, en l'occurrence les États-Unis, est admise a priori. Il ne faut pas perdre de vue que, si ce raisonnement peut trouver une justification en l'espèce dans le caractère démocratique des États-Unis, cela ne signifie pas qu'il pourrait être applicable et transposable aux relations avec tout autre pays tiers.

61. Selon l'annexe du rapport du HLCG, tout transfert de données à caractère personnel doit être pertinent, nécessaire et approprié. Le CEPD souligne que, pour être proportionné, le traitement ne doit pas être inutilement intrusif et que les modalités du traitement doivent être équilibrées et tenir compte des droits et intérêts des personnes concernées.

62. C'est pourquoi l'accès aux informations ne devrait être autorisé qu'au cas par cas, en fonction des besoins pratiques d'une enquête spécifique. L'accès permanent des autorités répressives d'un pays tiers aux bases de données situées dans l'UE serait considéré comme disproportionné et insuffisamment justifié. Le CEPD rappelle que, même

([22]) Voir notamment l'article 7, points c) et e), de la directive 95/46/CE. Dans son avis n° 6/2002 du 24 octobre 2002 sur la transmission aux États-Unis d'informations relatives aux passagers et d'autres données par les compagnies aériennes, le Groupe «Article 29» a déclaré qu'«il ne paraît pas acceptable qu'une décision unilatérale d'un pays tiers pour des raisons d'intérêt public qui lui sont propres conduise au transfert régulier et massif de données protégées par la directive».

dans le cadre des accords existants sur l'échange de données, tels que l'accord PNR, cet échange est lié à des circonstances précises et est limité dans le temps ([23]).

63. Selon la même logique, la durée de conservation des données devrait être réglementée: les données devraient être conservées aussi longtemps que nécessaire, en fonction de la finalité spécifique poursuivie. Si elles ne sont plus pertinentes au regard de la finalité déclarée, elles devraient être effacées. Le CEPD est fermement opposé à la constitution de stocks de données dans lesquels seraient conservées des informations concernant des personnes non suspectes en vue de pouvoir répondre à un éventuel besoin ultérieur.

4. Sécurité de l'information

64. Les principes prévoient des mesures et des procédures visant à protéger les données contre l'utilisation abusive, l'altération et d'autres risques, ainsi qu'une disposition limitant l'accès aux personnes autorisées, ce que le CEPD juge satisfaisant.

65. Ce principe pourrait en outre être complété par une disposition prévoyant la tenue de registres des personnes qui consultent les données. L'efficacité des garanties destinées à limiter l'accès aux données et à prévenir leur utilisation abusive s'en trouverait ainsi renforcée.

66. Par ailleurs, il conviendrait de prévoir une information mutuelle en cas d'atteinte à la sécurité: les destinataires situés aux États-Unis et ceux situés dans l'UE seraient tenus d'informer leurs homologues de toute divulgation illicite de données qui leur ont été transmises. Cela contribuerait à une responsabilité accrue aux fins de la sécurisation du traitement des données.

5. Catégories particulières d'informations à caractère personnel

67. Le principe de l'interdiction du traitement des données sensibles est, selon le CEPD, considérablement affaibli par l'exception qui autorise tout traitement de données sensibles pour lequel la législation interne prévoit des «garanties appropriées». En raison justement du caractère sensible des données, toute dérogation au principe d'interdiction doit être justifiée de manière adéquate et précise, au moyen d'une liste décrivant les finalités poursuivies et les circonstances dans lesquelles un type particulier de données sensibles peut être traité, ainsi que la qualité des responsables autorisés à traiter ces données. Parmi les garanties à adopter, le CEPD considère que les données sensibles ne devraient pas constituer en tant que telles un élément susceptible de déclencher une enquête. Elles pourraient être accessibles dans des circonstances spécifiques, mais uniquement en tant qu'informations complémentaires concernant une personne faisant déjà l'objet d'une enquête. Ces garanties et conditions doivent être bien délimitées dans l'énoncé du principe.

6. Obligation de rendre des comptes

68. Comme expliqué aux points 55 et 56 du présent avis, il convient de veiller à ce que l'obligation de rendre des comptes soit imposée de manière effective aux organismes publics qui traitent des données à caractère personnel, l'accord devant donner des assurances à ce sujet. Le manque de transparence qui entoure généralement le traitement de données à caractère personnel dans un contexte répressif rend le respect de cette obligation d'autant plus important. À cet égard, le fait d'indiquer — comme c'est le cas actuellement dans l'annexe 6 que les organismes publics sont tenus de rendre des comptes, sans donner davantage d'explication sur les modalités et les conséquences de cette obligation, ne constitue pas une garantie satisfaisante. Le CEPD recommande d'ajouter une explication à ce propos dans le dispositif de l'instrument.

7. Supervision indépendante et efficace

69. Le CEPD soutient sans réserve l'inclusion d'une disposition prévoyant une supervision indépendante et efficace par une ou plusieurs autorités de contrôle. Il estime qu'il conviendrait de préciser ce que l'on entend par «indépendance», en indiquant notamment par rapport à qui ces autorités seraient indépendantes et sous la responsabilité de qui elles seraient placées. Il convient, à cet égard, de définir des critères qui tiennent compte de l'indépendance institutionnelle et fonctionnelle des autorités de contrôle par rapport aux organes exécutifs et législatifs. Le CEPD rappelle qu'il s'agit d'un élément essentiel pour garantir le respect effectif des principes fixés d'un commun accord. Les pouvoirs d'intervention et de répression de ces autorités sont également fondamentaux au regard de l'obligation de rendre des comptes imposée aux organismes publics qui traitent des données à caractère personnel, comme expliqué ci-dessus. Les personnes concernées devraient recevoir des informations claires sur l'existence et les compétences de ces autorités afin de pouvoir exercer leurs droits, en particulier si plusieurs autorités sont compétentes en fonction du contexte du traitement.

70. Par ailleurs, le CEPD recommande de prévoir également dans un futur accord des mécanismes de coopération entre les autorités de contrôle.

8. Accès individuel et rectification

71. Des garanties spécifiques sont nécessaires en ce qui concerne l'accès et la rectification dans un contexte répressif. Dans cette optique, le CEPD est favorable au principe selon lequel les particuliers doivent/devraient avoir accès aux informations à caractère personnel les concernant et pouvoir en obtenir la rectification et/ou l'effacement. Toutefois, certaines incertitudes subsistent quant à la définition des «particuliers» (toutes les personnes concernées devraient être protégées, et pas seulement les citoyens du pays concerné) et aux conditions dans lesquelles ceux-ci peuvent s'opposer au traitement

([23]) L'accord expirera et cessera de produire ses effets sept ans après la date de la signature, sauf si les parties conviennent mutuellement de le remplacer.

des informations les concernant. Des précisions sont nécessaires à propos des «cas appropriés» dans lesquels une objection peut ou non être formulée. Les personnes concernées devraient savoir clairement dans quelles circonstances — selon, par exemple, le type d'autorité, le type d'enquête ou d'autres critères — elles pourront faire valoir leurs droits.

72. Par ailleurs, s'il n'existe pas de possibilité directe de s'opposer à un traitement pour des raisons justifiées, une vérification indirecte devrait être possible, par l'intermédiaire de l'autorité indépendante responsable de la supervision du traitement.

9. Transparence et information

73. Le CEPD souligne une nouvelle fois qu'il est important de garantir une transparence effective, afin de permettre aux particuliers d'exercer leurs droits et de contribuer au respect de l'obligation générale de rendre des comptes imposée aux autorités qui traitent des données à caractère personnel. Il approuve les principes tels qu'ils sont énoncés et insiste en particulier sur la nécessité d'une information générale et individuelle des personnes concernées, conformément au principe figurant au point 9 de l'annexe.

74. Néanmoins, au chapitre 2, point B, intitulé «Agreed upon principles» («Principes fixés d'un commun accord»), il est indiqué que, aux États-Unis, la transparence «peut inclure, individuellement ou conjointement, la publication au Registre fédéral, l'information individuelle et la divulgation dans le cadre d'une procédure judiciaire» (traduction du Conseil). Il convient de préciser qu'une publication au journal officiel ne suffit pas à garantir l'information appropriée de la personne concernée. Outre la nécessité d'une information individuelle, le CEPD rappelle que l'information doit être fournie sous une forme et dans des termes aisément compréhensibles par la personne concernée.

10. Recours

75. Pour pouvoir exercer effectivement leurs droits, les particuliers doivent avoir la possibilité d'introduire une réclamation auprès d'une autorité indépendante compétente en matière de protection des données et de former un recours devant un tribunal indépendant et impartial. Ces voies de recours devraient être toutes les deux offertes aux intéressés.

76. L'accès à une autorité indépendante compétente en matière de protection des données est nécessaire car celle-ci offre une assistance souple et moins coûteuse, dans un contexte — la répression — qui peut revêtir un caractère assez opaque pour les particuliers. Les autorités responsables de la protection des données peuvent également apporter leur concours en exerçant le droit d'accès au nom des personnes concernées, lorsque des exceptions empêchent ces dernières d'obtenir un accès direct aux données à caractère personnel les concernant.

77. L'accès au système judiciaire est un moyen supplémentaire et indispensable de garantir aux personnes concernées la possibilité de former un recours auprès d'une autorité appartenant à une branche du système démocratique distincte des institutions publiques qui traitent effectivement leurs données. Cette voie de recours effective devant une juridiction a été considérée par la Cour de justice des Communautés européennes ([24]) comme «essentielle pour assurer au particulier la protection effective de son droit. (...) [Elle] constitue un principe général de droit communautaire qui découle des traditions constitutionnelles communes aux États membres et qui a trouvé sa consécration dans les articles 6 et 13 de la Convention européenne des droits de l'homme». L'existence d'une voie de recours juridictionnelle est également prévue explicitement à l'article 47 de la Charte des droits fondamentaux de l'Union européenne, ainsi qu'à l'article 22 de la directive 95/46/CE, sans préjudice d'éventuels recours administratifs.

11. Décisions individuelles automatisées

78. Le CEPD accueille favorablement la disposition prévoyant des garanties appropriées en cas de traitement automatisé d'informations à caractère personnel. Il fait observer qu'une interprétation commune de l'expression «effets significatifs préjudiciables aux intérêts pertinents du particulier» (traduction du Conseil) apporterait des éclaircissements quant aux conditions d'application de ce principe.

12. Transferts ultérieurs

79. Les conditions fixées pour le transfert ultérieur sont, pour certaines d'entre elles, peu claires. En particulier, lorsque le transfert ultérieur doit respecter des accords internationaux et des accords entre le pays d'origine et le pays destinataire, il convient de préciser s'il s'agit des accords entre les deux pays ayant organisé le premier transfert ou des deux pays concernés par le transfert ultérieur. Selon le CEPD, un accord entre les deux pays ayant organisé le premier transfert est en tout état de cause nécessaire.

80. Le CEPD note également que la définition des «intérêts publics légitimes» autorisant un transfert ultérieur est très large. Le champ couvert par la sécurité publique est flou, et l'extension des transferts aux cas de manquements aux règles de déontologie de professions réglementées semble injustifié et excessif dans un contexte répressif.

VI. **CONCLUSION**

81. Le CEPD salue le travail conjoint réalisé par les autorités de l'UE et celles des États-Unis dans le domaine répressif, où la protection des données est cruciale. Il tient toutefois à souligner que la question est complexe, notamment en ce qui concerne sa portée et sa nature précises, et qu'elle requiert dès lors une analyse minutieuse et approfondie.

([24]) Affaire 222/84, *Johnston*, Recueil 1986, p. 1651; affaire 222/86, *Heylens*, Recueil 1987, p. 4097; affaire C-97/91, *Borelli*, Recueil 1992, p. I-6313.

L'impact d'un instrument transatlantique sur la protection des données devrait être soigneusement examiné au regard du cadre juridique existant et de ses conséquences pour les citoyens.

82. Le CEPD préconise davantage de clarté et de dispositions concrètes, en particulier pour ce qui concerne les aspects suivants:

— il convient de préciser la nature de l'instrument, qui devrait être juridiquement contraignant afin d'offrir une sécurité juridique suffisante;

— il convient de réaliser une analyse approfondie de l'adéquation, sur la base des exigences essentielles portant sur les aspects du système relatifs au contenu, à la spécificité et à la supervision. Le CEPD estime que l'instrument général ne peut être considéré comme adéquat que s'il est complété par des accords spécifiques appropriés, au cas par cas;

— un champ d'application bien délimité et une définition claire et commune des finalités répressives poursuivies sont nécessaires;

— il convient de préciser les modalités selon lesquelles des organismes privés pourraient être impliqués dans le cadre de transferts de données;

— le principe de proportionnalité doit être respecté: les échanges de données doivent avoir lieu au cas par cas, pour répondre à un besoin concret;

— des mécanismes de surveillance solides sont nécessaires, et les personnes concernées doivent disposer de voies de recours, y compris de recours administratifs et juridictionnels;

— des mesures effectives doivent garantir à toutes les personnes concernées la possibilité d'exercer leurs droits, indépendamment de leur nationalité;

— il convient de prévoir la participation d'autorités indépendantes compétentes en matière de protection des données, notamment en ce qui concerne la supervision et l'assistance aux personnes concernées.

83. Le CEPD insiste sur le fait qu'il convient d'éviter toute précipitation dans l'élaboration des principes, sous peine d'aboutir à des solutions insatisfaisantes dont les effets seraient contraires à ceux recherchés en termes de protection des données. La meilleure voie à suivre au stade actuel serait donc d'établir une feuille de route en vue d'un éventuel accord ultérieur.

84. Le CEPD préconise également une plus grande transparence dans le processus d'élaboration des principes relatifs à la protection des données. La participation de tous les acteurs concernés, y compris le Parlement européen, est une condition sine qua non pour que l'instrument fasse l'objet d'un débat démocratique profitable et obtienne le soutien et la reconnaissance nécessaires.

Fait à Bruxelles, le 11 novembre 2008.

Peter HUSTINX

Contrôleur européen de la protection des données