
Rocco Bellanova et Paul De Hert

Protection des données personnelles et mesures de sécurité : vers une perspective transatlantique

Avertissement

Le contenu de ce site relève de la législation française sur la propriété intellectuelle et est la propriété exclusive de l'éditeur.

Les œuvres figurant sur ce site peuvent être consultées et reproduites sur un support papier ou numérique sous réserve qu'elles soient strictement réservées à un usage soit personnel, soit scientifique ou pédagogique excluant toute exploitation commerciale. La reproduction devra obligatoirement mentionner l'éditeur, le nom de la revue, l'auteur et la référence du document.

Toute autre reproduction est interdite sauf accord préalable de l'éditeur, en dehors des cas prévus par la législation en vigueur en France.

revues.org

CENTRE POUR L'ÉDITION ÉLECTRONIQUE OUVERTE
CENTRE FOR OPEN ELECTRONIC PUBLISHING

Revues.org est un portail de revues en sciences humaines et sociales développé par le CLEO, Centre pour l'édition électronique ouverte (CNRS, EHESS, UP, UAPV).

Référence électronique

Rocco Bellanova et Paul De Hert, « Protection des données personnelles et mesures de sécurité : vers une perspective transatlantique », *Cultures & Conflits* [En ligne], Tous les numéros, Sécurité et protection des données, mis en ligne le 28 octobre 2010. URL : <http://conflits.revues.org/index17429.html>

DOI : en cours d'attribution

Éditeur : Centre d'études sur les conflits

<http://conflits.revues.org>

<http://www.revues.org>

Document accessible en ligne à l'adresse suivante : <http://conflits.revues.org/index17429.html>

Ce document est le fac-similé de l'édition papier.

Licence creative commons

Protection des données personnelles et mesures de sécurité : vers une perspective transatlantique

Rocco BELLANOVA, Paul DE HERT

Rocco Bellanova fait partie du Centre de recherche en science politique aux Facultés universitaires Saint-Louis et du Centre de recherches Law, Science, Technology & Society à la Vrije Universiteit Brussel.

Paul De Hert fait partie du centre de recherches Law, Science, Technology & Society à la Vrije Universiteit Brussel et du Tilburg Institute for Law and Technology à la Tilburg University.

Lors du sommet UE-Etats-Unis de juin 2008, les « dirigeants de l'Union européenne et des Etats-Unis d'Amérique » déclaraient une préférence commune pour la conclusion d'un « *accord international contraignant* » entre Union européenne (UE) et Etats-Unis garantissant la protection de la vie privée et des données personnelles ¹. La déclaration du Conseil fait référence au Rapport final du Groupe de contact de haut niveau UE-Etats-Unis (*High Level Contact Group* ou HLCG) sur le partage des informations et la protection de la vie privée et des données à caractère personnel ². Les travaux du HLCG ont le double objectif de renforcer la coopération transatlantique dans le domaine du partage de données et d'informations tout en assurant les droits à la protection des données et au respect de la vie privée. Le rapport final a notamment répertorié les principes communs de la protection des données et du respect de la vie privée à des fins répressives ³, a trouvé un « langage commun » ⁴ et a aussi identifié les principales questions en suspens ⁵. Dans le

1. « Nous sommes conscients du fait que, pour lutter contre la criminalité et le terrorisme, il faut être en mesure de mettre en commun les données à caractère personnel à des fins répressives tout en protégeant pleinement les droits fondamentaux et les libertés civiles de nos citoyens, et notamment le respect de leur vie privée et de leurs données à caractère personnel grâce au maintien des normes nécessaires en matière de protection des données à caractère personnel. [...] La meilleure manière de sauvegarder ces intérêts communs est de recourir à un accord international contraignant portant sur toutes les questions recensées dans le rapport du HLCG. », Conseil de l'Union européenne, *Déclaration du Sommet UE-Etats-Unis de 2008*, doc. 10562/08 (Presse 168), Brdo, 10 juin 2008, p. 10.

même rapport, le HLCG a également avancé des options politiques principales visant à traduire les travaux exploratoires en produits réels.

Or, la déclaration du Conseil et les travaux du HLCG s'inscrivent dans un contexte transatlantique caractérisé à la fois par des poussées de coopération dans le domaine de la sécurité intérieure et l'accès aux données personnelles, et des tensions sur le respect des droits fondamentaux à la vie privée, à la protection des données et d'autres libertés civiles. Dans ce cadre, et compte tenu d'un relatif manque de littérature sur ce sujet, il paraît important d'esquisser une première étude sur les systèmes européen et américain de protection de données personnelles couvrant les activités de justice et affaires intérieures (le soi-disant troisième pilier). Cette analyse n'a aucune prétention à l'exhaustivité, compte tenu des limites implicites à la matière, au contexte et à la nature de la recherche même. Malgré cela, l'objectif est de contribuer à la réflexion et à la discussion sur les solutions qui garantiraient une meilleure protection des droits des individus.

L'étude se divise en deux parties. La première offre un aperçu du système européen couvrant le troisième pilier, tout en soulignant les principes qui le soutiennent ainsi que son caractère fragmentaire et dispersé. La seconde se focalise sur le système nord-américain, analysé dans une perspective européenne, avec le but d'en identifier les différences structurelles et de contenu. Dans la partie conclusive, nous avancerons des recommandations pour de futurs travaux transatlantiques.

-
2. Conseil de l'Union européenne, *EU-US Summit, 12 June 2008. Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection*, doc. 9831/08, Bruxelles, 28 mai 2008, p. 2.
 3. Le projet de rapport final du groupe de contact à haut niveau répertorie 12 principes communs de la protection des données et du respect de la vie privée à des fins répressives. Ces principes sont : (i) Spécification de la finalité/Limitation de la finalité ; (ii) Intégrité/Qualité des données ; (iii) Pertinent et nécessaire/Proportionnalité ; (iv) Sécurité de l'information ; (v) Catégories particulières d'informations à caractère personnel (données sensibles) ; (vi) Responsabilité ; (vii) Surveillance indépendante et efficace ; (viii) Accès et rectification par l'individu ; (ix) Transparence et avis ; (x) Recours ; (xi) Décisions individuelles automatisées ; (xii) Restrictions sur les retransferts vers des pays tiers (doc. 9831/08, pp. 4 et 11-14).
 4. Toutefois, le Groupe de contact à haut niveau lui-même introduit quelques remarques sur ce langage commun. La première série de spécifications concerne les principes 7 et 9. En fait, « surveillance indépendante et efficace » doit être compris comme l'accomplissement de l'effet désiré plutôt qu'une exécution parallèle du même principe. « Transparence et avis » doit être compris comme « les informations qui devraient être mises à la disposition des personnes concernées », et les droits nationaux détermineront les modalités des informations et leurs limitations. Cependant, la plus importante remarque du Groupe de contact à haut niveau concerne le principe de recours. Même si les deux côtés partagent l'idée que les personnes concernées doivent avoir un accès réel à toute procédure de recours, il existe de fortes différences dans les deux systèmes juridiques en ce qui concerne l'accès aux recours juridiques.
 5. Ces questions sont : (i) Cohérence des obligations des entités privées pendant les transferts de données ; (ii) Application équivalente et réciproque de la législation relative à la protection de la vie privée et des données à caractère personnel ; (iii) Eviter un impact excessif sur les relations avec les pays tiers ; (iv) Accords spécifiques réglementant l'échange des informations et la protection de la vie privée et des données à caractère personnel ; (v) Questions liées au cadre institutionnel de l'UE et des Etats-Unis (doc. 9831/08, pp. 7 et 14).

1. Principes de la protection des données dans l'UE

Législation et grands principes européens relatifs aux activités du troisième pilier

La protection de la vie privée au niveau européen est principalement régie par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales de 1950 et l'article 7 de la Charte des droits fondamentaux de l'Union européenne de 2000. En outre, la protection des données dans l'UE est régie par la directive 95/46/CE 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 (la dénommée « directive relative à la protection des données »), par la directive 2002/58/CE relative à la protection de la vie privée et au secteur des communications électroniques, par l'article 8 de la Charte des droits fondamentaux de l'Union européenne et par la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de 1981 (la dénommée « Convention n°108 »)⁶.

En dépit d'une abondante législation en matière de respect de la vie privée et de protection des données, le cadre législatif européen semble devenir, lorsque l'on en vient aux activités du troisième pilier, plus complexe et moins cohérent. Dans le contexte d'une utilisation croissante des technologies de l'information et d'une tendance vers un accès mutuel aux bases de données privées et publiques, la structure à piliers européenne constitue un obstacle majeur à la définition d'un cadre plus efficace. En effet, le principal document de la législation européenne sur la protection des données – la Directive relative à la protection des données de 1995 – n'est valable que pour le champ d'application du droit communautaire (directive 95/46/CE art. 3(2)). De plus, comme cela a été souligné par la Cour de justice dans son arrêt PNR, la directive relative à la protection des données ne s'applique pas au traitement des données collectées en premier lieu par des acteurs privés et auxquelles on accède ensuite à des fins de sécurité publique⁷. Cet aspect est encore plus inquiétant, car il risque de permettre l'accès des autorités publiques à des données commerciales dans une sorte de *no man's land*⁸. Plusieurs lois tentent de

6. Sur les différences entre protection de la vie privée et protection des données personnelles, voir : De Hert P., Gutwirth S., "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power", in E. Claes, A. Duff, S. Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp/Oxford, Intersentia, 2006, pp. 61-104 ; De Hert P., Gutwirth S., "Regulating Profiling in a Democratic Constitutional State", in Hildebrandt M., Gutwirth S. (eds.), *Profiling the European Citizen*, Springer, Dordrecht, 2008, pp. 278-280.

7. Voir : Cour européenne de Justice, *Parlement européen c. Conseil de l'Union européenne* (C-317/04) et Commission des Communautés européennes (C-318/04), Affaires jointes C-317/04 et C-318/04. Rapports de 2006 de la Cour européenne Page I-04721.

8. Voir De Hert P., Papakonstantinou V., Riehle C., "Data Protection in the Third Pillar: Cautious Pessimism", in Mike M. (ed.), *Crime, Rights and the EU: The Future of Police and Judicial Cooperation*, Justice, Londres, 2008, p. 180.

compenser l'absence d'un cadre approprié en fournissant des dispositions *ponctuelles* de protection des données dans leurs textes. Dès lors, malgré le fait que le traitement lié à la sécurité en Europe ne possède pas de base réglementaire commune, des secteurs spécifiques sont allés de l'avant : plus particulièrement l'accord de Schengen ⁹, mais aussi les accords Europol ¹⁰ et Eurojust ¹¹, qui incluent tous des règles et des procédures détaillées en matière de protection des données dans leurs textes respectifs. Par conséquent, ce qui est réellement en place actuellement au sein de l'UE en ce qui concerne le traitement du troisième pilier est une série d'approches spécifiques au secteur qui coexistent avec la Convention du Conseil de l'Europe sur la protection des données de 1981 ¹² et la décision-cadre relative à la protection des données sous le troisième pilier (DCPD), approuvé en décembre 2008.

Parmi les autres instruments qui forment ce patchwork législatif, il est important de mentionner :

- les règles de législation nationale et la surveillance nationale fournie par les autorités chargées de la protection des données indépendantes ;

- les règles de protection des données *ponctuelles* d'une série d'initiatives répressives, tant au niveau européen, comme la décision du Conseil de Prüm, qu'au niveau transatlantique, comme les accords PNR et SWIFT ;

- les règles de protection des données *ponctuelles* des agences européennes ou au niveau de l'UE : Eurojust et Europol ; ainsi que les règles de protection des données de l'accord transatlantique entre Europol et les États-Unis ¹³ ;

- la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, en particulier l'article 8, et la jurisprudence relative de la Cour européenne des droits de l'homme ;

- la Charte des droits fondamentaux de l'Union européenne, dès que le Traité de Lisbonne entrera en vigueur.

9. Se référant en fait à Schengen I (Accord entre les Gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française, relatif à la suppression graduelle des contrôles aux frontières communes, entré en vigueur en 1985) et Schengen II ou CIS (Convention de l'application de l'Accord de Schengen du 14 juin 1985 entre les Gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française, relatif à la suppression graduelle des contrôles aux frontières communes, entrée en vigueur en 1990).

10. Voir la Convention EUROPOL (texte consolidé) sur www.europol.europa.eu/index.asp?page=legal

11. Voir Décision du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité (2002/187/JAI), JO L 63/L.

12. Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, STE n°108, Strasbourg, 18 janvier 1981.

La Convention 108 constitue toujours la base juridique de la protection des données couvrant les activités du troisième pilier. Bien que ses principes généraux soient toujours valables, il est important de noter qu'elle a été rédigée avant le développement massif des technologies de l'information. Si elle n'est pas intégrée ou remplacée au niveau de l'UE par un nouveau cadre, elle risque de devenir obsolète et d'être dépassée par l'application croissante d'instruments technologiques ¹⁴. Ce fait explique, par exemple, les règles de protection des données élaborées dans la Convention Europol qui complètent la Convention 108, et la récente initiative européenne de rédiger un (nouveau) cadre général relatif à la protection des données dans le cadre du troisième pilier.

La décision-cadre du 27 novembre 2008 relative à la protection des données dans le cadre du troisième pilier

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 a été finalement approuvée en décembre 2008 ¹⁵. Compte tenu de la récente adoption de cet instrument, ainsi que de son rôle potentiel dans la protection des données personnelles, il est important d'offrir un aperçu de son contenu.

L'article 1(1) énonce l'objet de la DCPD :

« garantir à la fois un niveau élevé de protection des droits et libertés fondamentaux des personnes physiques, en particulier leur droit au respect de la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale [...] et un niveau élevé de sécurité publique ».

L'article 1(2) définit le champ d'application de la DCPD. Les données à caractère personnel couvertes par cet instrument sont des données qui sont

13 . Par exemple, l'initiative remarquable de transfert des données à caractère personnel aux Etats-Unis sur la base de la Convention Europol, voir : De Hert P., De Schutter B., "International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and SWIFT", in Martenczuk B., van Thiel S. (eds.), *Justice, Liberty and Security: New Challenges for EU External Relations*, VUB Press, Bruxelles, 2008.

14 . Voir De Hert P., Papakonstantinou V., Riehle C., *op. cit.*

15 . Décision-Cadre du Conseil 2008/977/JHA, JO L/350/60, 30 décembre 2008. L'approbation de la DCPD est l'aboutissement d'un long processus de négociations, commencé avec la présentation du projet de proposition de décision-cadre par la Commission européennes en 2005. Plusieurs changements ont été apportés au texte initial, en raison de la difficulté des Etats membres à trouver un terrain commun ainsi que des critiques avancées par le Parlement européen et le Contrôleur européen de la protection des données. Jusqu'à présent, le CEPD a soumis trois opinions différentes sur trois versions différentes de la DCPD : JO C/2006/47/27 ; JO C/2007/91/9 et JO C/2007/139/1, et, lors de l'approbation, un commentaire.

transmises aux Etats membres ou mises à leur disposition, tout comme aux autorités et aux systèmes d'information établis sur la base du Titre VI du Traité sur l'Union européenne, ou reçues ou mises à disposition par celui-ci. De plus, l'article 1(3) limite le champ d'application :

« au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ».

Enfin, l'article 1 laisse aux Etats membres la possibilité de fournir des garanties plus élevées pour la protection des données à caractère personnel collectées ou traitées au niveau national.

Les définitions clés des termes dans la décision-cadre sont reprises à l'article 2. Parmi celles-ci, il est utile de noter la définition plutôt détaillée du « *fichier de données à caractère personnel* » incluant un « *ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique* » (art. 2(d)).

Les articles 3-6, 8, 10 et 16-22 définissent et abordent les principaux principes de protection des données. En particulier, l'article 3 traduit les principes de légitimité, de proportionnalité et de finalité. Il soumet également le « *traitement ultérieur* » au respect des mêmes principes. L'article 4 prévoit les principes de rectification, d'effacement et de blocage. L'article 5 établit les délais relatifs à l'effacement et la révision. L'article 6 définit les règles de traitement des catégories particulières de données. ..L'article 8(1) demande à l'autorité compétente de prendre « *toutes les mesures raisonnables pour faire en sorte que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour ne soient pas transmises ou mises à disposition* ». Il garantit par conséquent le principe de qualité des données. L'article 10 prévoit l'obligation de collecte et de documentation, contribuant à aborder le principe de transparence.

Les articles 16 à 20 prévoient des droits aux personnes concernées : information ; accès ; rectification, effacement et blocage ; compensation ; recours judiciaire. Les articles 21 et 22 assurent les principes de confidentialité et de sécurité de traitement.

Le rôle et les pouvoirs des autorités de contrôle nationales sont décrits aux articles 23 et 25. L'article 25 prescrit que les autorités de contrôle nationales

16 . Les données régies par l'article 6 sont celles « *révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale [...]* [et] *les données relatives à la santé ou la vie sexuelle* ». Même si ces catégories rappellent et

doivent avoir les pouvoirs d'enquêter, d'intervenir et de s'engager dans des poursuites judiciaires.

Cet aperçu des principaux principes semble confirmer que la décision-cadre reflète le même principe que la Convention n°108 et la Directive 95/46/EC. Cependant, une analyse plus étroite révèle certaines différences, comme celle qui concerne les données sensibles et les droits d'accès aux données ¹⁶. L'article 14 sur la transmission des données à caractère personnel aux parties privées est d'un intérêt particulier. Par son existence même, cette disposition semble confirmer l'idée d'une interaction, et d'une intégration, croissante des bases de données privées et publiques dans la gestion de la sécurité.

Les règles relatives au transfert des données à caractère personnel aux Etats tiers (article 13) sont particulièrement pertinentes pour cette étude, tout comme la relation avec les accords avec les pays tiers (article 26). L'article 13(1) définit les conditions de transmission, et en particulier le besoin du consentement préalable de l'Etat membre qui est à l'origine de la transmission ou de la mise à disposition des données (article 13(1)(c)) et une sorte de recherche d'adéquation ponctuelle (« *l'Etat tiers ou l'instance internationale concerné assure un niveau de protection adéquat pour le traitement de données envisagé* », article 13(1)(d)). Cependant, ce cadre strict de protection des données est affaibli par les paragraphes suivants. L'article 13(2) permet un transfert sans consentement préalable, si celui-ci est essentiel à la prévention d'une menace sérieuse et immédiate. En outre, le considérant 24 allège encore le consentement préalable en laissant à chaque Etat membre la possibilité de déterminer les modalités de ce consentement, y compris un consentement général pour les catégories d'information ou pour les Etats tiers spécifiés. L'article 13(3) stipule qu'il est possible de déroger au critère d'adéquation si :

« (a) la législation nationale de l'Etat membre qui transfère les données le prévoit (i) pour des intérêts spécifiques légitimes de la personne concernée, ou (ii) lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants, ou (b) l'Etat tiers ou l'instance internationale destinataire prévoit des garanties qui sont jugées adéquates par l'Etat membre concerné conformément à sa législation nationale ».

Enfin, l'article 26 et le considérant 38 sur la relation vis-à-vis des accords avec les Etats tiers veillent à que la décision-cadre soit sans préjudice de toute obligation et de tout engagement découlant d'accords bilatéraux et/ou multilatéraux déjà existants. Ainsi, restent exclus de la portée de la décision-cadre

respectent la formulation de l'art. 6 de la Convention n°108 du Conseil de l'Europe, il est important de noter que la formulation a été « inversée ». En ce qui concerne les droits d'accès aux données, ceux-ci sont limités à l'art. 17(2), lequel introduit la possibilité de créer d'autres restrictions par les Etats membres.

tous les accords sécuritaires déjà conclus, tels que les accords PNR avec les Etats tiers (États Unis, Canada et Australie) ou le Traité de Prüm.

2. Principes de la protection des données aux Etats-Unis

Respect de la vie privée et protection des données dans le droit constitutionnel américain

La première couche de protection de la vie privée aux Etats-Unis se trouve au niveau constitutionnel fédéral. Bien que la Constitution des Etats-Unis ne se réfère pas explicitement au respect de la vie privée, les premier, troisième, quatrième et cinquième amendements offrent plusieurs formes de protection contre l'intrusion gouvernementale dans la vie des individus¹⁷. C'est surtout le quatrième amendement qui a fourni, et continue de fournir, la principale référence constitutionnelle à la protection de la vie privée aux Etats-Unis. Dans l'affaire *Schmerber c. Californie*, en 1966, la Cour suprême a déclaré que « [l]a fonction primordiale du quatrième amendement est de protéger la vie privée et la dignité contre l'intrusion injustifiée de l'Etat¹⁸ ».

Toutefois, l'application du quatrième amendement n'est pas sans problème, en raison de l'interprétation de sa formulation dans le contexte moderne des développements technologiques¹⁹. L'utilisation par la Cour suprême du critère des « *attentes raisonnables en matière de protection de la vie privée* » semble surtout – et ce contrairement à l'utilisation de celui-ci par la Cour européenne des droits de l'homme – nier la protection constitutionnelle dans la plupart des cas. Après un « début » prometteur du critère dans l'affaire *Katz*²⁰, il y a eu une longue série d'affaires dans lesquelles aucune protection constitutionnelle n'a été accordée aux questions du respect de la vie privée, par exemple dans l'affaire dite du *Pen Register* (enregistreur gra-

17. Congrès des Etats-Unis, *Bill of Rights* (déclaration des droits), 1789, Ier amendement. Disponible sur : http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html

18. *Schmerber c. Californie*, 384 U.S. 757, 767, 1966.

19. Gellman R., "A General Survey of Video Surveillance Law in the United States", in Nouwt S. et al. (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, T.M.C. Asser Press, 2005, p. 11 ; Breuner S., "Constitutional Rights and New Technologies in the United States", in Leenes R., Koops B.J., De Hert P., *Constitutional Rights and New Technologies. A Comparative Study*, T.M.C. Asser Press, 2008.

20. L'affaire *Katz c. Etats-Unis* (1967) est pertinente par rapport à deux questions : l'importance de l'individu et des relations entre l'individu, la société et le secteur privé. La Cour a souligné le principe que le quatrième amendement « *protège les personnes, pas les lieux* » (voir Solove D.J., Rotenberg M., Schwartz P.M., *Information Privacy Law*, 2e éd., Aspen, New York, 2006, pp. 34-35), s'axant dès lors sur l'individu plutôt que sur l'« *inviolabilité du domicile* ». Justice Harlan, participant à l'affaire *Katz*, a d'abord défini le fameux « *test des attentes raisonnables en matière de protection de la vie privée* » en vue de fournir une méthode pour déterminer le droit au respect de la vie privée des individus. Le test est double : une personne doit « *avoir formulé une attente réelle (subjective) en matière de protection de la vie privée* » et « *l'attente [doit] être une attente que la société est prête à reconnaître comme raisonnable* » (voir Solove et al., *op. cit.*, p. 34).

prique)²¹. La récente affaire *Kyllo* semble toutefois suggérer qu'une application plus constructive du critère, conformément à l'affaire *Katz* et à la jurisprudence de la Cour européenne des droits de l'homme, est encore possible²².

Bien que la vie privée ne soit pas seulement protégée d'une manière indirecte, il est utile de noter qu'en 1965, dans l'affaire *Griswold c. Connecticut*²³, la cour a déclaré que l'individu a un droit constitutionnel au respect de la vie privée. La protection des données à caractère personnel n'est pas assurée en tant que telle, et gardant à l'esprit l'affaire *Pen Register* et d'autres affaires, il serait mensonger de dire que les données à caractère personnel sont protégées en tant que telles par la Constitution sans qu'il y ait d'importants aspects relatifs au respect de la vie privée.

Enfin, il est important d'observer que le constitutionnalisme fédéral coexiste avec le constitutionnalisme d'Etat et qu'il est complété par celui-ci. Le droit constitutionnel au respect de la vie privée est directement assuré dans les constitutions de certains Etats. Parmi celles-ci, le droit constitutionnel californien au respect de la vie privée s'applique également aux parties privées²⁴.

21. Les défis soulevés par la double détermination *Katz* du droit au respect de la vie privée d'un individu sont clairement représentés par cette affaire, connue sous *Smith c. Maryland* (442 U.S. 735, 1979). Elle soutient que l'installation d'un dit « *pen register* » (enregistreur graphique), un dispositif mécanique qui enregistre les numéros composés sur un téléphone, ne violait pas le quatrième amendement même si elle était effectuée sans mandat. En fait, « *tous les utilisateurs de téléphone réalisent qu'ils doivent communiquer les numéros de téléphone à la compagnie de téléphone [...]. Tous les abonnés réalisent, en outre, que la compagnie de téléphone possède les équipements qui permettent l'enregistrement des numéros qu'ils composent* » (voir *Smith c. Maryland*, cité par Solove et al., *op. cit.*, p. 234). Etant donné l'utilisation quotidienne de ces équipements électroniques, notamment pour la prévention des infractions, l'attente raisonnable en matière de protection de la vie privée du requérant ne pouvait pas être considérée comme une attente que la société est prête à reconnaître comme raisonnable. Cependant, un tel raisonnement, basé sur une prétendue « *acceptation des risques* » pourrait devenir très problématique dans les sociétés contemporaines fortement basées sur les réseaux de communication, et dépendantes de ceux-ci.

22. Dans l'affaire *Kyllo c. Etats-Unis* (533, U.S. 141, 2000), la Cour a décidé que l'utilisation par le gouvernement d'un imageur thermique sans mandat est illégale, car la technologie n'est pas utilisée par le grand public. Dans ces cas, on devrait se pencher sur la question de savoir si « *les pères [fondateurs] ont apprécié ce niveau de sécurité découlant de la surveillance et du harcèlement du gouvernement* » (Ku R., cité dans Solove et al., *op. cit.*, p. 261).

23. Voir : *Griswold c. Connecticut*, 318 U.S. 479, 1965.

24. L'art. 1, sec. 1 de la Constitution californienne stipule : « *Tout individu est par nature libre et indépendant et possède des droits inaliénables. Parmi ceux-ci se trouvent la jouissance et la défense de la vie et de la liberté, l'acquisition, la possession et la protection des biens, ainsi que la poursuite et l'obtention de la sécurité, le bonheur et le respect de la vie privée* ». Il a été aussi établi un *Office of Privacy Information* et une nouvelle *Data Security Law* (loi sur la sécurité des données) est en cours d'élaboration, laquelle amenderait la loi sur l'avis de violation pour demander à ceux qui y sont soumis, les agences d'Etat et les personnes ou les entreprises exerçant en Californie, lorsqu'ils informent des individus d'une violation de leurs données à caractère personnel, tel que défini, d'informer également l'*Office of Privacy Protection*. Cela ne s'appliquerait que dans le cas de notifications effectuées par la méthode de « *substitution* », qui utilise les moyens de communication de masse plutôt que les notifications individuelles.

La protection des données est bien présente dans le paysage juridique américain. À partir des années 1960, la croissance des capacités et de la diffusion des technologies de l'information a fait l'objet d'une série de publications²⁵. La question principale devient, dès lors, la définition des garanties de protection de la gestion des données. Rédigé en 1973, le *Code of Fair Information Practices* est devenu la pierre angulaire de la législation ultérieure sur la protection des données²⁶. Il a identifié les cinq « pratiques » ou principes suivants : interdiction des systèmes secrets d'enregistrement des données ; possibilité d'accès pour l'individu à ces informations, principe de limitation de la finalité (sauf accord préalable), possibilité de correction des informations, principe de sécurité des informations²⁷.

Le principal document de la législation « dure » couvrant le traitement des données par les agences gouvernementales a été adopté l'année suivante, en 1974. Le *Privacy Act* (loi sur la protection de la vie privée)²⁸ est le principal cadre juridique protégeant les données à caractère personnel détenues par le secteur public aux Etats-Unis. Il protège les fichiers détenus par les agences gouvernementales américaines et leur demande d'appliquer des pratiques d'information justes²⁹. Il ressort d'un premier aperçu des dispositions principales du *Privacy Act* que le *Code of Fair Information Practices* a été largement intégré dans la formulation. Les cinq principes trouvent tous leur place dans la loi. Le principe de transparence est traduit au point (e)(4) : « *Chaque agence qui entretient un système de fichiers devra [...] publier dans le registre fédéral, lors de l'établissement ou de la révision, un avis d'existence et la nature du système de fichiers...* ». Les principes d'accès et de correction façonnent les dispositions de la section (d) sur l'« accès aux fichiers ». La sécurité des données est abordée dans la section sur les « exigences d'agence », au point (e)(5) et (10). Enfin, le principe de limitation de la finalité est garanti au point (e)(1), qui sti-

25. Peter Blok se réfère à ces publications sous la « littérature d'alarme », voir Blok P., « Protection des données aux Etats-Unis », chap. 1, titre IV, in De Hert P. (éd.), *Manuel sur la vie privée et la protection des données*, Bruxelles, Éditions Politéia, feuillets mobiles, mise à jour n°7, 2001, p. 3.

26. Le Code a été proposé par le rapport de l'*United States Department of Health, Education, and Welfare* (HEW) (ministère de la Santé, de l'Éducation et du Bien-Être des Etats-Unis).

27. *U.S. Department of Health, Education, and Welfare* (ministère de la Santé, de l'Éducation et du Bien-Être des Etats-Unis), *Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and Rights of Citizens* (Comité consultatif du Secrétaire sur les systèmes automatisés de données à caractère personnel, les fichiers, les ordinateurs et les droits des citoyens), 1973, p. viii. Disponible sur : <http://epic.org/privacy/hew1973report/>. Voir aussi : Solove et al., *op. cit.*, pp. 35-36.

28. Voir : *Privacy Act* (loi sur la protection de la vie privée), 5 U.S.C. § 552a, 1974.

29. Après une première section dédiée à la définition des termes clés, les dispositions du *Privacy Act* définissent (entre autres) : les « conditions de divulgation » (§ 552a (b)) ; la « comptabilité de certaines divulgations » (c) ; l'« accès aux fichiers » (d) ; les « exigences d'agence » (e) ; les « recours civils » (g) ; les « sanctions pénales » (i) ; les « exceptions générales et spécifiques » (j et k) et les « comités d'intégrité des données » (u).

pule que chaque agence ne devra « *conserver dans ses fichiers que les informations concernant un individu qui sont pertinentes et nécessaires pour accomplir une finalité de l'agence qui doit être exécutée par une loi ou un décret présidentiel* ».

Outre la traduction des pratiques d'information justes, le *Privacy Act* identifie une catégorie particulière de données sensibles : « *les fichiers décrivant comment un individu exerce des droits garantis par le Premier amendement* » (e)(7). De tels fichiers ne seront pas conservés, sauf en cas de règles strictes et pertinentes. Le *Privacy Act* prévoit l'établissement de Comités d'intégrité des données au sein des agences participant à des programmes de correspondance ou conduisant ceux-ci (u). Ce Comité d'intégrité des données a essentiellement des pouvoirs de révision, d'approbation et de fixation des directives. Il n'a aucun pouvoir d'exécution et n'est pas indépendant d'un point de vue structurel, puisqu'il se compose de « *hauts fonctionnaires nommés par le chef de l'agence* » (u)(2).

Enfin, les sections (g) et (i) définissent les procédures de recours juridique à la disposition des individus et les sanctions pénales applicables pour certaines catégories de fautes commises par des fonctionnaires gouvernementaux.

Trois failles principales du Privacy Act d'un point de vue transatlantique

Malgré cette remarquable traduction des pratiques d'information justes dans la formulation du *Privacy Act*, un certain nombre d'intellectuels, tant européens que nord-américains, ont développé de très vives critiques³⁰. Vu la portée de cette étude, il est utile de concentrer l'analyse sur certaines des failles principales relevées dans le *Privacy Act*, en particulier celles qui pourraient constituer (ou constituent déjà) une question essentielle en cas de négociation d'un accord transatlantique³¹. Une des notions élémentaires du *Privacy Act* est le « système de fichiers », c'est-à-dire le « *groupe de tous les fichiers sous le contrôle d'une agence à partir duquel les informations sont retrouvées par le nom de l'individu ou par un certain numéro ou symbole d'identification, ou toute autre caractéristique d'identification attribuée à l'individu* »³². Selon un

30. Voir : Blok P., *op. cit.* ; Bignami F., "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data mining", *Boston College Law Review*, vol.48, 2007, pp. 609-698 ; Bignami F., *The U.S. Privacy Act in Comparative Perspective*, Contribution to the European Parliament Public Seminar "PNR/SWIFT/Safa Harbour: Are Transatlantic Data Protected?", 26 mars 2007, disponible sur : http://www.europarl.europa.eu/hearings/20070326/libe/bignami_en.pdf

31. En général, les détracteurs identifient au moins cinq séries de questions : le *Privacy Act* ne couvre qu'un nombre limité d'autorités (voir : Blok P., *op. cit.*) ; il fournit peu de limitations importantes à l'utilisation des données à caractère personnel (voir Blok P., *op. cit.*) ; l'attitude passive de l'*Office of Management and Budget* (Bureau de la gestion publique et du budget) (voir Blok P., *op. cit.*) ; les inefficacités et les limitations du système de recours (voir Blok P., *op. cit.*, Bignami F., *op. cit.*) et l'absence d'institutionnalisation d'une autorité indépendante (voir Bignami F., *op. cit.*).

32. Voir § 552a (a)(5)) du *Privacy Act* de 1974.

auteur, la définition actuelle du « système de fichiers », associée à l'utilisation d'un instrument d'extraction de données, pourrait entraîner l'exclusion de grandes bases de données du champ d'application du *Privacy Act* ³³. La disponibilité et la diffusion de l'extraction de données dans une action répressive pourraient entraîner l'établissement de nouvelles bases de données sortant du champ d'application du *Privacy Act*. De plus, une telle interprétation du « système de fichiers » pourrait renforcer les divergences dans l'interprétation de la collecte et du partage de données.

Le *Privacy Act* accorde certains droits à chaque « individu », en sachant qu'un « individu » est « *un citoyen des Etats-Unis ou un étranger légalement admis pour une résidence permanente* » ³⁴. Dans sa simplicité plutôt paradoxale, la question du recours – ou plutôt la non-disponibilité de recours civils aux citoyens non américains – constitue une des principales questions en jeu dans le suivi des travaux du Groupe de contact de haut niveau. En fait, selon la définition de l'« individu » rappelée ci-dessus, les citoyens européens qui ne sont pas permanents aux Etats-Unis sont exclus du champ d'application du *Privacy Act*. Cette disposition représente à elle seule un obstacle majeur dans les négociations transatlantiques ³⁵. Cependant, les dispositions relatives aux recours civils sont, *en soi*, formulées d'une manière qui limite fortement la possibilité du recours juridique. Pour intenter une action civile contre l'agence, le comportement de l'agence doit avoir eu un effet négatif sur l'individu (g)(1)(D). De plus, la Cour devrait déterminer si « *l'agence a agi d'une façon qui était intentionnelle ou délibérée* » (g)(4). Un cadre aussi complexe, surtout dans un contexte marqué par l'absence d'autorités structurelles indépendantes, risque de limiter *ex ante* l'exécution du recours juridique. En outre, le critère d'« effet négatif » pourrait être difficile à prouver dans un environnement marqué par l'utilisation de technologies de contrôle invisibles ³⁶.

La troisième série de questions concerne les limitations et les exceptions à la gestion des données imposées par le *Privacy Act*. L'interprétation administrative de la disposition permettant la divulgation des données « *pour un usage routinier* » ³⁷ a, selon les dires, *considérablement* diminué l'efficacité de la loi ³⁸.

33. Voir Bignami F, "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data mining", *op. cit.*, pp. 634-635.

34. Voir § 552a (a)(2) du *Privacy Act* de 1974.

35. Dans son avis sur le niveau d'adéquation de la protection offerte par le *Privacy Act*, la Commission belge de la protection de la vie privée a souligné les mêmes points (Commission de la protection de la vie privée, 1998, pp. 2-5).

36. Voir "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data mining", *op. cit.*, p. 633.

37. Voir § 552a (a)(7)) du *Privacy Act* de 1974. L'usage routinier « *signifie, en ce qui concerne la divulgation d'un fichier, l'utilisation de ce fichier dans une finalité qui est compatible avec la finalité pour laquelle il a été collecté* ».

Comme mentionné précédemment, les Etats-Unis ne possèdent pas de cadre juridique complet couvrant le secteur privé. Toutefois, depuis les années 1970, le Congrès a adopté plusieurs lois couvrant un secteur économique différent ou réglementant des activités de surveillance.

Ces lois pouvaient d'abord être axées sur des activités spécifiques, telles que la location de vidéos ³⁹, jusqu'à aborder une question plus transversale telle que l'évaluation du crédit ⁴⁰. Il est aussi important de mentionner le *Health Insurance Portability and Accountability Act* (HIPAA) de 1996 ⁴¹, qui accorde au ministère américain de la Santé et des Services sociaux le pouvoir de promulguer des réglementations sur le respect de la vie privée des dossiers médicaux ; le *Gramm-Leach-Bliley Act* (GLBA) de 1999 ⁴² qui oblige les institutions financières à publier des avis relatifs à la protection de la vie privée et à fournir des droits d'opposition lorsqu'elles cherchent à divulguer des données à d'autres sociétés ; ainsi que le *Children's Online Privacy Protection Act* de 1998 (Pub. L. No. 106-170, 15 U.S.C. §§ 6501-6569) qui restreint l'utilisation des informations collectées auprès d'enfants âgés de moins de 13 ans par des sites Internet.

Parmi les lois réglementant les activités de surveillance, il est utile de rappeler le *Foreign Intelligence Surveillance Act* (FISA) (loi sur le contre-espionnage) (50 U.S.C. §§ 1801-1811, 1978), amendé par l'*USA Patriot Act* de 2001, ainsi que l'*Electronic Communication Privacy Act* (loi de confidentialité des communications électroniques) ⁴³. Ces deux lois fournissent des normes et des procédures pour l'utilisation de la surveillance électronique, le FISA se concentrant sur la collecte de renseignements extérieurs. Il est utile de remarquer que les récents amendements apportés au FISA ont affaibli ses normes protectrices. L'*USA Patriot Act* a modifié la nécessité de collecter des renseignements extérieurs : d'une « *finalité première* » à une « *finalité significative* » ⁴⁴. L'importance potentielle de ces changements d'un point de vue transatlantique a été aussi remarquée par les hauts fonctionnaires européens impliqués dans les réunions Justice et affaires intérieures (JAI) informelles ⁴⁵.

38. Voir Electronic Privacy Information Center – EPIC, *Privacy and Human Rights, An International Survey of Privacy Laws and Developments*, USA, 2006, p. 1008 ; Blok P., *op. cit.*, pp. 22-23.

39. *Video Privacy Protection Act*, 18 U.S.C. §§ 2710-2711, 1988.

40. *Fair and Accurate Credit Transactions Act*, Pub. L. No. 108-159, 2003.

41. Voir : *Health Insurance Portability and Accountability Act* (HIPAA), Pub. L. No. 104-191, 1996.

42. Voir : *Gramm-Leach-Bliley Act* (GLBA), Pub. L. No. 106-102, 15 U.S.C. §§ 6801-6809, 1999.

43. 18 U.S.C. §§ 2510-2522, 2701-2709, 1986

44. Voir Electronic Privacy Information Center – EPIC, *Privacy and Human Rights, An International Survey of Privacy Laws and Developments*, *op. cit.*, p. 7 ; Solove D.J., et al., *op. cit.*, pp. 288-289.

45. Conseil de l'Union européenne, *EU-US informal JHA senior level meeting (09-10 janvier 2008, Ljubljana)*, doc. 5172/08, Bruxelles, 18 janvier 2008, pp. 5-6.

Le Congrès a également adopté d'autres lois qui traitent de la protection de la vie privée et des données, mais dans le but d'encourager l'accès du gouvernement aux données à caractère personnel ⁴⁶. Parmi celles-ci, l'une des plus significatives est l'*USA Patriot Act* ⁴⁷. Depuis son adoption, ce dernier a soulevé d'après discussions et critiques ⁴⁸, allant de l'affaiblissement des garanties de protection de la vie privée d'autres lois jusqu'à l'accusation visant à déséquilibrer la relation entre le gouvernement et l'individu. L'*USA Patriot Act* introduit de nombreuses réformes dont les suivantes : une nouvelle définition du terrorisme national ; un avis retardé des mandats de perquisition ; une nouvelle définition des enregistreurs graphiques (*Pen Registers*) et des dispositifs de traçage (*Trap and Trace devices*) ; le partage des renseignements extérieurs.

Une seconde loi importante traite de la protection de la vie privée et des données : le *Homeland Security Act* (loi sur la sécurité intérieure) ⁴⁹. Cette loi consolide et fusionne vingt-deux agences fédérales au sein d'un ministère américain de la Sécurité intérieure (*Department of Homeland Security*, DHS) et constitue un *Privacy Office* au sein du même ministère ⁵⁰.

Enfin, il est important de mentionner ici un autre document émanant de la législation américaine qui pourrait jouer un rôle essentiel dans la protection de la vie privée. Si, comme mentionné, l'accès aux fichiers et le recours juridique pourraient être limités pour les citoyens européens en vertu du *Privacy Act*, le *Freedom of Information Act* (FOIA) (loi relative à la liberté de l'information) ⁵¹ donne la possibilité à toute personne d'accéder aux fichiers tenus par les autorités publiques américaines. Toutefois, ce droit d'accès n'est pas sans limitations, surtout lorsque les informations traitent d'activités de répression (paragraphe (b)(7) et (c)(1)), de renseignements extérieurs et de contre-espionnage (c)(3) ⁵².

46. Pour une liste complète des lois adoptées depuis le début des années 1970 aux Etats-Unis, voir Solove D.J., et al., *op. cit.*, pp. 36-37. Pour de plus amples détails sur chaque législation, se reporter au chapitre approprié de la même publication.

47. *Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act – USA-PATRIOT Act* (loi d'union et de renforcement de l'Amérique pour fournir les outils appropriés nécessaires pour intercepter et faire obstacle au terrorisme). Pub. L. No. 107-56, 2001.

48. Voir : Electronic Privacy Information Center – EPIC, *Privacy and Human Rights, An International Survey of Privacy Laws and Developments*, *op. cit.*, p. 8 ; Solove D.J., et al., *op. cit.*, pp. 298-300 ; Birnhack M.D., Elkin-Koren N., "The Invisible Handshake: The Reemergence of the State in the Digital Environment", *Virginia Journal of Law and Technology*, vol.8, 2003, pp. 30-31.

49. Voir : *Homeland Security Act* (loi sur la sécurité intérieure), 6 U.S.C. § 222, 2002.

50. Le *Homeland Security Act* (loi sur la sécurité intérieure) de 2002 a établi le *DHS Privacy Office*. Le Secrétaire du DHS a la responsabilité de nommer un haut fonctionnaire au poste de *Chief Privacy Officer* (DHS CPO). Les responsabilités de ce *Chief Privacy Officer* sont de veiller à ce que l'utilisation des technologies soutiennent et n'érodent pas les protections de la vie privée ; d'assurer la conformité des systèmes de gestion des fichiers du *Privacy Act* aux pratiques d'information justes du *Privacy Act* ; d'évaluer les propositions de loi et de réglementation ; d'effectuer une évaluation de l'impact sur la protection de la vie privée et de faire un rapport tous les ans au Congrès.

3. Remarques conclusives

UE et Etats-Unis : deux partenaires ayant des principes communs mais des attitudes différentes ?

Une des images possibles pouvant rendre compte des relations Etats-Unis - UE peut être un chiasme : une législation générale dans l'UE en ce qui concerne le secteur privé, mais une approche progressive dans le troisième pilier ; une approche progressive dans le secteur privé aux Etats-Unis, mais une sorte de législation générale, le *Privacy Act*, couvrant le traitement gouvernemental des fichiers. Cette image est toujours valable, bien que de nouveaux développements législatifs soient de nature à la brouiller. Cela est particulièrement vrai du côté européen, où un déplacement s'opère vers un cadre plus général dans le domaine de la Justice et des Affaires intérieures, avec l'adoption de la décision-cadre relative à la protection des données. Cependant, la décision-cadre risque de ne pas régler de manière satisfaisante tous les problèmes et, en particulier, ceux qui sont liés au transfert des données vers les pays tiers.

Trois différences semblent prépondérantes d'un point de vue européen :

1. Le *Privacy Act* ne protège pas les individus qui ne sont pas soit des citoyens américains, soit des résidents permanents. Cette absence de protection constitue l'une des principales préoccupations pour toute négociation transatlantique.

2. L'absence d'autorités de contrôle chargées de la protection des données indépendantes aux Etats-Unis constitue certainement d'un point de vue européen un affaiblissement du système, surtout en cette période de développement technologique rapide.

3. L'absence d'une base juridique solide pour le principe de minimisation et de la limitation de la finalité dans le droit américain représente un troisième défaut important de la protection des données américaine dans le contexte de la dissémination croissante des données à caractère personnel dans la vie de tous les jours. Bien que de nombreux principes de protection de données tels que reconnus dans le droit européen soient présents dans le droit américain, il n'existe aucune base solide dans le droit américain pour ces principes essentiels.

51. Disponible sur : <http://www.usdoj.gov/oip/foiastat.htm> (5 U.S.C. § 552, dernièrement amendé en 2002).

52. Il est intéressant de noter qu'un membre néerlandais du Parlement européen, Sophie In't Veld, a décidé de tester le système FOIA en présentant une demande d'accès à ses données traitées par l'*Automatic Targeting System* (Système de ciblage automatique).

Il est aussi important de souligner que les mesures de sécurité se fondent de plus en plus sur l'implication du secteur privé et qu'elles dépendent du développement de pratiques « invisibles » d'analyse et de surveillance, telles que l'évaluation des risques, le profilage et la comparaison. Dans un tel contexte, il est difficile de maintenir une distinction claire entre la protection des données dans le secteur privé et dans le secteur public. Les données collectées pour une finalité pourraient devenir, en soi, des données pouvant être traitées à d'autres fins et dans un domaine différent. Cela souligne l'importance cruciale d'instruments juridiques capables tant de bloquer l'utilisation illégitime des données que de canaliser l'utilisation légitime des pouvoirs. Le rapport du HLCG a pris, justement, en considération des différences telles que le principe de recours et la supervision indépendante. Par contre, pour la réussite d'un futur accord, il serait aussi nécessaire d'avancer une solution au manque de base juridique solide pour les principes de minimisation et de limitation de finalité.

Quelle voie possible à terme ?

Dans ce contexte, la possible conclusion d'un accord transatlantique sur l'échange et la protection des données personnelles est à la fois « *bienvenue et délicate* », comme cela a été souligné par le Contrôleur européen de la protection des données⁵³. Compte tenu des caractéristiques, des failles des deux systèmes et des options suggérées par le groupe de contact de haut niveau, la meilleure solution serait l'adoption d'un accord juridiquement contraignant. Cet accord entraînerait donc un effet direct concernant les critères minimaux de protection de données, à intégrer au cas par cas, par des mesures ponctuelles.

53. Voir : CEPD, *Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact group on information sharing and privacy and personal data protection*, Bruxelles, 11 novembre 2008, p. 2.

54. L'UE ne devrait pas seulement aborder la question du recours pour les citoyens non américains. Le champ d'application limité du recours américain (« effet négatif intentionnel ») est tout aussi difficile. Il rejette l'idée européenne de base selon laquelle la préoccupation relative à la protection des données n'est pas seulement de bloquer et de poursuivre l'utilisation illégitime des données, mais aussi de canaliser l'utilisation légitime des données et de créer un recours pour les problèmes qui se présentent à cet égard (voir : De Hert P., Gutwirth S., « Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power », *op. cit.*).

55. Dans ses négociations avec les Etats-Unis, l'UE devra se montrer très prudente dans ses exigences et formulations. Les adresses IP et les autres données à caractère personnel telles que des images CCTV peuvent ne pas être considérées comme des données à caractère personnel par les fonctionnaires américains (voir Gellman R., « A General Survey of Video Surveillance Law in the United States », in Nouwt S. et al. (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, T.M.C. Asser Press, 2005).

56. Par ailleurs, même si le Parlement européen n'a pas participé directement au groupe de contact à haut niveau, il semble avoir déjà exprimé une préférence pour la conclusion d'un accord international « *assurant un contrôle démocratique et parlementaire approprié au niveau national et au niveau de l'Union* » (Parlement européen, *Résolution du Parlement*

Ainsi, le but des négociations devrait être d'assurer à la fois les droits de recours aux citoyens européens, ainsi que la possibilité d'être représentés par leur autorité en charge de la protection des données. Une telle possibilité pourrait considérablement rétablir les effets négatifs des procédures d'auto-assistance : contraintes financières et temporelles ainsi que la connaissance généralement limitée d'un système juridique étranger ⁵⁴.

Etant donné son importance dans le système américain, les négociations européennes doivent aborder le champ d'application de notions telles que « *données à caractère personnel* » ⁵⁵ ainsi que le besoin d'incorporer des principes tels que la minimisation des données, ou encore les difficultés pour les citoyens non américains à obtenir un recours juridique. Bien que de nombreux principes de protection des données tels que reconnus dans le droit européen soient présents dans le droit américain, il n'existe aucune base solide dans ce dernier pour des principes essentiels comme la limitation de la finalité et la minimisation des données. La protection de ces principes essentiels devrait être un élément central des négociations européennes.

D'un point de vue institutionnel, le Parlement européen devrait soutenir et participer directement aux négociations d'un accord contraignant ⁵⁶. Le Contrôleur européen de la protection des données a déjà rendu public son avis sur le rapport final du HLCG ⁵⁷, et lui aussi devrait participer directement aux travaux, comme cela se passe aux Etats-Unis, où le *Chief Privacy Officer* a déjà été intégré à ce groupe.

Non seulement le Parlement européen doit être entièrement impliqué dans la conclusion d'un accord relatif à l'échange de données entre l'UE et les Etats-Unis, mais il serait également important d'inviter le Congrès et le Sénat américains à participer. Cela pourrait s'avérer particulièrement essentiel, dans l'éventualité où des changements législatifs seraient nécessaires du côté américain, notamment pour étendre la protection du *Privacy Act* aux citoyens européens.

européen du 12 décembre 2007 sur la lutte contre le terrorisme, doc. P6_TA(2007)0612, Strasbourg, 12 décembre 2007). Du même avis paraît être aussi le Coordinateur pour l'UE de la lutte contre le terrorisme. Dans son rapport au Conseil sur la mise en œuvre de la stratégie de l'UE visant à lutter contre le terrorisme, il déclare qu'« il semble qu'un accord juridiquement contraignant entre l'UE et les Etats-Unis (à négocier sur la base du traité de Lisbonne) offrirait les meilleures garanties en termes de protection des données et d'intensification durable de l'échange de données en matière de répression » (Conseil de l'Union européenne, *Mise en œuvre de la stratégie de l'UE visant à lutter contre le terrorisme – les priorités des actions futures*, doc. 9417/08, Bruxelles, 19 mai 2008).

57. Voir : CEPD, *Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact group on information sharing and privacy and personal data protection*, op. cit.

Finalement, en ce qui concerne la portée de l'accord contraignant, il faut souligner qu'il restera toujours le besoin de conserver des instruments clairs de canalisation des pouvoirs légitimes et de blocage de l'utilisation illégitime, surtout si on considère les nouveaux défis posés par les nouvelles mesures de sécurité. Or, un accord « *one-fits-all* », permettant tout type d'échange de données, ne pourrait pas devenir un cadre de référence convaincant pour les années à venir.