



Brugge

College of Europe
Collège d'Europe



Natolin

Le cadre européen de protection des données personnelles en matière pénale Dimensions interne et externe

Carole Pouliquen



DEPARTMENT OF EUROPEAN POLITICAL
AND ADMINISTRATIVE STUDIES

Bruges Political Research Papers

29 / 2013



College of Europe
Collège d'Europe

Brugge



Natolin

European Political and Administrative Studies /
Études Politiques et Administratives

Bruges Political Research Papers / Cahiers de recherche politique de Bruges
No 29 / May 2013

Le cadre européen de protection des données personnelles en matière pénale
Dimensions interne et externe

Par Carole Pouliquen

© Carole Pouliquen, 2013

European Political and Administrative Studies /
Études Politiques et Administratives
Dijver 11, B-8000 Brugge, Belgium
www.coleurope.eu/pol

A propos de l'auteur:

Carole est diplômée de Sciences Po Strasbourg et de la Faculté de Droit de Strasbourg, avec une spécialisation dans les problématiques de Justice et Affaires Intérieures. Par la suite, elle a été diplômée du Collège d'Europe à Bruges, Belgique, dans la filière études politiques et administratives européennes. Elle travaille actuellement à Bruxelles.

Contact : carole.pouliquen@coleurope.eu

Editorial Team

Michele Chang, Claire Baffert, Thibaud Deruelle, Marie Eichholtzer, Mateusz Grzelczyk, Rossella Marangio, Nathalie Rubin-Delanchy, Amaia Zabala Aldunate, and Jörg Monar
Dijver 11, B-8000 Bruges, Belgium | Tel. +32 (0) 50 477 281 | Fax +32 (0) 50 477 280
email michele.chang@coleurope.eu | website www.coleurope.eu/pol

Views expressed in the Bruges Political Research Papers are solely those of the author(s) and do not necessarily reflect positions of either the series editors or the College of Europe. If you would like to be added to the mailing list and be informed of new publications and department events, please email rina.balbaert@coleurope.eu. Or find us on Facebook: College of Europe Politics and Administration Department. European Political and Administrative Studies

Résumé

L'intervention européenne pour assurer la protection des données personnelles quand elles sont utilisées à des fins répressives est relativement récente. Cette étude analyse le cadre mis en place par l'Union européenne (UE) pour faire cohabiter sécurité publique, traitement des données personnelles, et respect de la protection de ces données. Les dimensions interne et externe de ce cadre sont exposées, pour réfléchir non seulement au degré de protection des données personnelles offert par l'UE, mais également pour étudier la cohérence entre la protection offerte au niveau interne, et celle offerte au niveau externe.

Cette recherche débute en expliquant que l'UE est parvenue à élaborer sa propre conception de la protection des données en matière pénale, et se poursuit en confrontant cette conception à son application concrète, tant pour la coopération policière et judiciaire en matière pénale (dimension interne) que pour la lutte contre le financement du terrorisme (dimension externe).

Introduction

«Ceux qui sont prêts à abandonner une liberté essentielle en échange d'un peu de sécurité ne méritent ni la liberté, ni la sécurité» (Benjamin Franklin). Souvent perçus comme antinomiques, sécurité et liberté sont pourtant deux biens publics essentiels au bon fonctionnement de toute société. Outre le fait qu'elles doivent cohabiter, ces deux notions entretiennent un lien étroit avec les données à caractère personnel (ci-après, données personnelles).

Au titre de leurs libertés fondamentales, les citoyens européens détiennent le droit à la protection de leurs données personnelles. Au titre de la sécurité publique, l'UE a cherché à construire une politique sécuritaire englobant la création d'un Espace de Liberté, de Sécurité et de Justice (ELSJ) d'une part (dimension interne), et la lutte contre le terrorisme d'autre part (dimension externe). Les données personnelles, essentielles au travail des autorités répressives, font constamment l'objet d'échanges entre les Etats membres, mais également entre l'UE et les pays tiers.

Cette étude s'attachera à explorer ces deux dimensions pour analyser le cadre global mis en place par l'UE en matière de protection des données personnelles utilisées à des fins répressives.

Deux questions se posent alors: l'UE est-elle parvenue à «dissoudre» la tension entre sécurité publique et protection des données personnelles dans sa législation pour la coopération policière et judiciaire en matière pénale, et dans l'accord signé avec les Etats-Unis en matière de la lutte contre le financement du terrorisme? Les garanties offertes aux citoyens européens pour la protection de leurs données sont-elles similaires si les données sont utilisées par les autorités répressives des Etats membres, ou si elles sont utilisées par les Etats-Unis à des fins de lutte contre le financement du terrorisme?

Pour répondre à ces questions, 1.) il est nécessaire tout d'abord de poser le cadre conceptuel que l'Union utilise pour traiter la question des données personnelles en matière pénale. La comparaison de la mise en œuvre de cette conception pour chacune des deux dimensions requiert 2.) une analyse du cadre interne; 3.) et passe par l'examen du cadre externe, via le Terrorist Finance Tracking Programme, dans le domaine spécifique du contre-terrorisme.

1. La protection des données personnelles en matière pénale: exposé d'une conception propre à l'Union européenne

Vingt-sept autorités répressives différentes ne peuvent coopérer efficacement sans un degré minimum d'harmonisation des règles relatives à la coopération policière et judiciaire en matière pénale. L'échange de données personnelles constitue l'un des aspects de cette coopération pour lequel l'élaboration de standards communs est un prérequis indispensable à la protection de ces données. Ces standards communs n'ont pas été décidés arbitrairement. Ils relèvent d'une conception unique et propre à l'UE. Cette conception passe en premier par la reconnaissance par l'UE de la protection des données personnelles en tant que droit fondamental.

1.1 La protection des données: un droit fondamental

Nous devons la première reconnaissance du droit à la protection des données personnelles à la Cour européenne des Droits de l'Homme (CEDH). Alors que la Convention de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales (CESDH) ne mentionne pas ce droit en tant que tel, la CEDH s'est appuyée sur l'article 8 de la CESDH, qui donne droit «au respect de la vie privée et familiale».¹ Dans l'affaire «Lander contre

¹ Conseil de l'Europe, *Convention européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales*, Série des traités du Conseil de l'Europe n° 005, Rome, 4 novembre 1950, article 8, p. 11.

Suède»,² elle a reconnu que le traitement des données personnelles pouvait porter atteinte au droit au respect de la vie privée. De ce fait, les traitements de données personnelles entrent pour la CEDH, dans le cadre de l'article 8 de la Convention de 1950, ce qui consacre la protection des données comme un droit fondamental.

Malgré cette reconnaissance, l'UE a jugé utile de développer son propre texte de référence. Proclamée et signée le 7 décembre 2000,³ la Charte des droits fondamentaux approfondit le processus engagé par la CEDH dans la mesure où son article 8 est dédié à la protection des données personnelles⁴ (voir infra). La Charte obtient avec le traité de Lisbonne force contraignante,⁵ symbole fort de la place accordée à la protection des données dans l'UE.

1.2 Sécurité et libertés fondamentales: quel terrain d'entente?

Ce débat philosophique oppose classiquement les tenants des libertés fondamentales, aux défenseurs de toujours plus de sécurité, pour lesquels des sacrifices doivent être consentis pour assurer la sécurité.

L'intervention de l'UE permettrait «d'apaiser ce débat» en encadrant l'usage des données personnelles par les forces de police, ce qui assurerait aux citoyens leur sécurité et le respect de leur vie privée. Cependant, une question persiste: à quelles limitations des droits individuels «la société est-elle prête à consentir pour accroître son niveau de sécurité collective et individuelle?»⁶ Les dérogations à ce droit fondamental ne doivent être permises seulement si certaines conditions sont remplies, conditions qui ne doivent en aucun cas

² CEDH, 26 mars 1987, «Lander contre Suède», série A, n°116, §48.

³ «La charte des droits fondamentaux», Parlement européen, consulté le 13 avril 2012, http://www.europarl.europa.eu/charter/default_fr.htm

⁴ L. Coudray, *La protection des données personnelles dans l'Union européenne, Naissance et consécration d'un droit fondamental*, Editions universitaires européennes, Editions universitaires européennes, Saarbruck, 2010, p. 290 et Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, 28 Janvier 1981, Série des traités européens, n° 108.

⁵ *Ibid.*, p. 289. Voir également article 6 TUE.

⁶ A. Türk, P. Piazza, La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée, Cultures et Conflits, Fichage et Listing, n° 76, hiver 2009, p. 124.

contredire l'essence même de ce droit fondamental,⁷ et que l'UE va tenter de définir et de mettre en place, tant dans la dimension interne, régie par le principe de disponibilité, qu'en externe.

Au titre de la cohérence entre l'action intérieure et extérieure de l'UE, on pourrait penser que la conception de l'UE en matière de protection des données personnelles s'applique également pour la coopération anti-terroriste avec les Etats-Unis. On retrouve dans cette coopération la même tension que pour la dimension interne entre sécurité et liberté. En revanche, l'écart qui sépare les standards de protection des données aux Etats-Unis et les standards appliqués au niveau européen rend difficiles les négociations entre les deux parties. Ces difficultés peuvent être illustrées par la signature de l'accord Terrorist Tracking Finance Programme («accord TFTP»).

1.3 Contenu de la conception

L'UE s'est tout d'abord inspirée de la Convention 108 du Conseil de l'Europe,⁸ qui réglemente l'usage automatisé des données personnelles et établit des normes strictes pour la collecte et le traitement des données personnelles, tant pour le secteur privé que pour le secteur public. La Convention fixe au titre de son article 5, les cinq principes que les données doivent satisfaire pour que leur traitement respecte le droit à la protection des données.

Les données en elles-mêmes doivent respecter les principes de «proportionnalité»⁹ et d'«exactitude».¹⁰ La collecte doit se faire de manière «licite» et «loyale».¹¹ Par ailleurs, le principe de finalité posé dans l'article 5 alinéa b de la Convention, stipule que les données ne

⁷ S. Rodota, «Data protection as a fundamental right», dans *Reinventing Data Protection?*, S. Gutwirth, Y. Poullet, P. de Hert (dir.), 2011, Dodrecht: Springer, p. 81.

⁸ N. Deffains, Traitement de données à caractère personnel et droit au respect de la vie privée devant la Cour européenne des droits de l'homme, Techniques et droit humain, Actes du Colloque organisé du 20 au 23 avril 2010, Montchrestien 2011, p. 253.

⁹ E. De Busser, EU data protection in transatlantic cooperation in criminal matters: Will the EU be serving its citizens an American meal?, *Utrecht Law Review*, Volume 6, Issue 1, 2010, p. 5.

¹⁰ Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 Janvier 1981, Série des traités européens, n° 108, article 5, §d.

¹¹ *Ibid.*, §a.

peuvent être utilisées que dans le but d'atteindre les finalités recherchées et préalablement définies.¹²

Ces cinq principes sont complétés par des droits accordés à la personne concernée par le traitement des données, tel que le droit à l'information ou à la rectification.¹³ En revanche, les dérogations permises par la Convention au titre de son article 9, affaiblissent cette protection. Si un Etat partie à la Convention invoque la «sûreté de l'Etat», la «sécurité publique» ou encore «la répression des infractions pénales», il peut déroger aux principes posés par l'article 5.¹⁴

L'interprétation de ces moyens de dérogation constitue l'un des éléments qui a conduit l'UE à reconnaître un droit spécifique à la protection des données personnelles dans sa Charte des droits fondamentaux, en établissant une distinction entre le droit au respect de la vie privée (article 7) et le droit à la protection des données personnelles (article 8). Depuis l'entrée en vigueur du traité de Lisbonne, la Charte ne se résume plus à n'être qu'une source d'inspiration, puisque les futures législations de l'UE en la matière devront respecter les principes posés par la Charte et ne pourront ainsi pas entraver ni le droit au respect de la vie privée, ni le droit à la protection des données personnelles.¹⁵

Les échanges de données personnelles entre les autorités répressives des vingt-sept Etats membres sont régis par la décision-cadre de 2008,¹⁶ signe que l'UE a tardé à prendre en compte la spécificité du traitement des données personnelles en matière pénale.

¹² De Busser, *op. cit.*, p. 94.

¹³ Convention 108, article 8, §a et c, *op. cit.*, p. 5.

¹⁴ *Ibid.*, p. 6.

¹⁵ A. Davoli, *La protection des données à caractère personnel*, Parlement européen, Fiche technique 4.12.8, mars 2011.

¹⁶ Conseil de l'Union européenne, Décision-cadre (2008/977/JAI) du 27 novembre 2008, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350 du 30 décembre 2008.

2. La mise en œuvre de la conception européenne de protection des données personnelles en matière pénale: perspective interne

Adoptée en 2008, la décision-cadre régit les échanges de données personnelles entre les autorités répressives des vingt-sept Etats membres de l'UE. Alors que l'UE est parvenue à élaborer sa propre conception de la protection des données personnelles en matière pénale, parvient-elle à la transposer dans sa législation? Pour répondre à cette question, il faut tout d'abord expliquer comment le cadre juridique de l'UE en matière de protection des données personnelles a-t-il fini par prendre en compte la spécificité de la Coopération policière et judiciaire en matière pénale (CJPP).

2.1 Reconnaissance progressive de la spécificité du traitement des données personnelles en matière pénale

Jusqu'en 2008, aucun texte ne régissait spécifiquement la protection des données personnelles en matière pénale. La directive 95/46/CE régissait la protection des données personnelles, mais seules les matières relevant de l'ancien pilier étaient couvertes,¹⁷ et la Convention 108 ne reconnaît pas expressément la spécificité de la CPJP.¹⁸ Les débats relatifs à la nécessité de réglementer l'utilisation des données dans le secteur de la police ont émergé au Conseil de l'Europe en 1987.¹⁹ Au niveau de l'UE, ce n'est qu'en 2004 que l'eurodéputé Marco Cappato a soulevé le problème en demandant à la Commission de présenter un projet «d'instrument légal sur la protection de la vie privée dans le domaine relevant du troisième pilier».²⁰ Cependant, sous le régime du traité de Nice, seuls le Conseil et la Commission pouvaient décider de l'adoption d'un instrument spécifique. Les attentats de Londres

¹⁷ Parlement Européen et Conseil, Directive (95/46/CE) 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, article 3§2, JO L 281 du 23 novembre 1995.

¹⁸ Convention 108, *op. cit.*, article 3, p. 4.

¹⁹ Conseil de l'Europe, Recommandation n° 87 (15), du Comité des Ministres aux Etats Membres, Visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, 17 septembre 1987, lors de la 410^{ème} réunion des Délégués des Ministres.

²⁰ Parlement européen, Rapport sur le premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE), Marco Cappato, 24 février 2004, A5-0104/2004, p. 7.

conduiront la Commission à proposer le 4 octobre 2005 la création d'une décision-cadre relative à la protection des données personnelles dans le cadre de la CPJP.²¹ Le Parlement européen a rapidement critiqué la direction prise par le débat au Conseil qui selon lui, menaçait gravement la protection des données personnelles.²² Le Conseil pour sa part avait affirmé sa volonté de trouver un accord sur le texte avant la fin 2007.²³

Face à l'opposition du Parlement européen, la Présidence allemande fit la promesse à Marine Roure, rapporteur de ce texte pour la Commission LIBE,²⁴ que les standards contenus dans la proposition de décision-cadre ne seraient pas inférieurs à ceux de la Convention 108 du Conseil de l'Europe. Le débat sera relancé par la présidence portugaise et aboutira à la fin de l'année 2007 à un accord politique relatif à la décision-cadre.²⁵

Entre 2005 et 2007, le Contrôleur Européen de la Protection des Données (CEPD) a continuellement soulevé les problèmes rencontrés au regard des standards contenus dans les textes amendés par le Conseil.²⁶ Pour lui, les textes proposés étaient incompatibles avec la Convention 108. Statewatch partageait ces critiques, qui estimait que le Conseil avait favorisé les intérêts des autorités répressives, car le texte était discuté au Conseil par le Groupe Pluridisciplinaire sur le Crime Organisé, dont l'objectif principal était d'aboutir à

²¹ Commission des Communautés européennes, 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, COM(2005) 475 final, Bruxelles, 4 octobre 2005.

²² Parlement européen, Rapport contenant une proposition de recommandation du Parlement européen à l'intention du Conseil sur l'évolution des négociations sur la décision-cadre sur la protection des données dans le cadre de la coopération policière et judiciaire en matière pénale, 14 décembre 2006, P6_TA(2006)0602.

²³ «Update on a Council framework decision on the protection of personal data», European Digital Rights, 20 Juin 2007, consulté le 6 avril 2012, <http://www.edri.org/edriagram/number5.12/framework-decision-data-protection>.

²⁴ «Protection des données personnelles dans le cadre de la coopération policière et judiciaire pénale: une proposition à hauts risques», EU-logos, 9 mai 2007, consulté le 10 avril 2012, http://www.eu-logos.org/eu-logos_nea-say.php?idr=4&idnl=440&nea=25&lang=fra&lst=0

²⁵ D.A. Blas, «First pillar and third pillar : need for a common approach on data protection?», in *Reinventing Data Protection?*, S. Gutwirth, Y. Pouillet, P. de Hert (dir.), 2011, Dodrecht: Springer, p. 228.

²⁶ CEPD, Avis du 19 décembre 2005 (Avis du contrôleur européen de la protection des données sur la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité, JO C47 du 25 février 2006), Avis du 29 novembre 2006 (Second opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, JO C91 du 26 avril 2007) et Avis du 27 avril 2007 (Troisième avis du contrôleur européen de la protection des données sur la 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, JO C139, du 23 juin 2007).

une situation où la libre circulation des données entre les différentes autorités répressives n'était pas empêchée par les droits relatifs à la protection des données.²⁷

A la fin de l'année 2007, alors que la décision-cadre n'était toujours pas adoptée, les Etats membres reconnaissent, par la signature du traité de Lisbonne et la rédaction de la déclaration 21 annexée au traité, que des règles régissant la protection des données personnelles et la libre circulation des données «pourraient s'avérer nécessaires».²⁸ Ainsi, la voie était ouverte à l'adoption de la décision-cadre.

2.2 La décision-cadre: la concrétisation de l'approche européenne de la protection des données en matière pénale?

Dans la décision-cadre de 2008, le Conseil a méthodiquement inscrit les principes de la Convention 108 et de la Charte des droits fondamentaux tout en les adaptant au domaine sensible de la CPJP. L'article 3§1 reprend les principes de licéité, proportionnalité et de finalité. Il est néanmoins possible aux autorités compétentes nationales de déroger au principe de finalité,²⁹ si cela sert la sécurité publique,³⁰ ou «la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière, ou l'exécution de sanctions pénales».³¹

Les droits de la personne concernée sont également établis dans les articles 16 à 20, qui dispose ainsi du droit à l'information, du droit d'accès, du droit à un recours, et du droit à l'effacement de ses données. Ici encore, le droit d'accès à l'information peut être limité par les Etats membres pour des impératifs de sécurité publique.

La décision-cadre permet également aux autorités répressives de déroger à l'obligation d'effacer ou de verrouiller les données lorsque le délai indiqué par l'autorité qui

²⁷ Statewatch, Observatory on data protection in the EU, consulté le 13 avril 2012, <http://www.statewatch.org/eu-dp.htm>

²⁸ Déclaration 21 annexée à l'acte final de la Conférence intergouvernementale qui a adopté le Traité de Lisbonne, signé le 13 décembre 2007, JO C 83 du 30 mars 2010.

²⁹ 2008/977/JAI, article 3, §2, *op. cit.*

³⁰ *Ibid.*, article 11c.

³¹ *Ibid.*, article 11a.

transmet les données est écoulé, ou si les données «sont nécessaires pour une enquête en cours, la poursuite d'infractions pénales ou l'exécution de sanctions pénales».³²

De surcroît, la décision-cadre connaît des problèmes de mise en œuvre. Comme le montre le rapport de mise en œuvre de novembre 2011 publié par la Commission,³³ sur les vingt-six Etats ayant envoyé les informations, quatorze ont indiqué avoir mis en œuvre la décision-cadre, alors que neuf devaient toujours prendre des mesures d'application, et n'avaient donc que partiellement mis en œuvre la décision-cadre.³⁴ Trois d'entre eux ont indiqué ne pas avoir transposé la décision-cadre: la Grèce, l'Italie et Chypre.³⁵

Enfin, la transposition dans les dispositifs législatifs nationaux montre que l'information des personnes concernées par les autorités répressives «fait l'objet de trop nombreuses limitations dans la grande majorité des Etats membres».³⁶ Alors que la décision-cadre poursuivait un objectif d'harmonisation des législations existantes, sa mise en œuvre conduit à instaurer différents standards de protection des données au sein même de l'UE,³⁷ ce qui laisse à penser que la décision-cadre n'incarne finalement que partiellement la conception européenne de protection des données en matière pénale.

2.3 La communication de janvier 2012: vers une intégration plus complète de la conception européenne de la protection des données en matière pénale dans la législation?

Dans sa communication de janvier 2012, la Commission propose de remplacer la décision-cadre par une directive qui régirait le traitement des données personnelles par les autorités compétentes dans le but de prévenir et détecter les infractions pénales, d'enquêter et

³² *Ibid.*, article 9, §1.

³³ Commission européenne, Rapport de la Commission fondé sur l'article 29, paragraphe 2, de la décision-cadre du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, COM(2012) 012 final, 25 janvier 2012, JO C102/38 du 5 avril 2012.

³⁴ *Ibid.*, p. 3.

³⁵ *Ibid.*

³⁶ *Ibid.*, p. 6.

³⁷ *Ibid.*, p. 2.

de poursuivre en la matière ou d'exécuter des sanctions pénales³⁸. Cette communication présente de nombreuses similarités avec la décision-cadre de 2008, car la philosophie de la nouvelle proposition repose en partie sur les mêmes fondements que ceux utilisés en 2008. En effet, la nouvelle proposition cherche à «protéger les libertés et droits fondamentaux des personnes physiques, et notamment leur droit à la protection des données à caractère personnel, et assurer l'échange de ces données entre autorités compétentes au sein de l'Union».³⁹ Par ailleurs les principes clés de la protection des données issus de la Convention 108 sont repris dans la nouvelle proposition.

Elle offre cependant de nouvelles clauses qui tendent à rééquilibrer la relation entre sécurité et protection des données. La nouvelle proposition introduit les opérations de traitement nationales dans le champ d'application du texte. Cette disposition peut être déduite de la formulation de l'article 2 «La présente directive s'applique au traitement de données à caractère personnel effectué par les autorités compétentes»,⁴⁰ car si la proposition ne mentionne ni les opérations de traitement purement nationales, ni les opérations de traitement transfrontières, c'est qu'elle s'applique aux deux.

Néanmoins, le texte n'est pas exempt de dérogations relatives au droit à l'information de la personne concernée au titre de l'article 11§4, ou encore au droit d'accès à l'information (article 13). Il s'agit dans l'ensemble des mêmes dérogations que celles prévues par la décision-cadre de 2008, ce qui est toutefois susceptible de remettre en cause les avancées discutées. Le CEPD reconnaît ainsi les avancées de cette proposition pour la protection des données en Europe, mais déplore que les règles relatives à la police et à la justice soient

³⁸ Commission européenne, *Communication relative à la protection de la vie privée dans un monde en réseau, Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle*, COM(2012) 9 final, Bruxelles, le 25 janvier 2012, p. 4.

³⁹ Commission européenne, Proposition de directive du Parlement européen et du Conseil, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM(2012) 10 final, Bruxelles, le 25 janvier 2012, p. 7.

⁴⁰ *Ibid.*, article 2, §1.

inadaptées.⁴¹ Malgré ces critiques, la proposition de la Commission tendrait à se rapprocher de la conception européenne étudiée en première partie.

Quel est l'avenir de cette proposition? Les amendements contenus dans le projet de rapport de l'eurodéputé Dimitrios Droustas (GR, PSE) publié le 20 décembre 2012 relèvent clairement le niveau de protection fixé dans la proposition de la Commission.⁴² Ainsi, le rapporteur explique que «les exceptions globales et généralisées ne sauraient donc être acceptées», «la notion de compatibilité d'utilisation doit être interprétée de manière restrictive», et juge indispensable qu'un mécanisme d'évaluation de la nécessité et de la proportionnalité soit introduit pour éviter que toutes les données soient systématiquement analysées.⁴³ Le rapport pointe également du doigt que certaines exceptions, si appliquées de manière trop laxiste, pourraient conduire aux transferts en masse des données vers les pays tiers.⁴⁴ Plus globalement, le rapporteur dénonce le fait que certaines dispositions de la proposition de directive n'offrent pas un niveau de protection équivalent à celui contenu dans la proposition de règlement.⁴⁵

Pour le moment, seule une réunion du groupe de travail DAPIX au Conseil, en charge de la protection des données personnelles, a eu lieu en février et aucune position officielle du Conseil n'a encore été annoncée. Cependant, d'après un membre du Secrétariat du Conseil, les Etats Membres seraient relativement opposés aux dispositions du rapport qui selon eux aggraverait les défauts de la proposition de la Commission.⁴⁶ D'après les Etats Membres, le système que le rapporteur Droustas souhaite mettre en place est irréaliste et ne pourrait fonctionner. Alors que la Commission LIBE du Parlement n'a pas encore voté le texte, il

⁴¹ P. Hustinx, Newsletter du CEPD, n°31, 28 janvier 2012, p. 3.

⁴² Parlement européen, Projet de rapport sur la proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, PE501.928v02-00.

⁴³ *Ibid.*, p. 112.

⁴⁴ *Ibid.*, p. 113.

⁴⁵ *Ibid.*, p. 114.

⁴⁶ Entretien avec un Haut Fonctionnaire, Secrétariat Conseil de l'UE, DG H, Bruxelles, 22 février 2013.

semble très probable que le Conseil refuse le texte en l'état. L'avenir de ce texte reste donc incertain. Pour sa part, le rapporteur Droustas a clairement appelé le Conseil à «s'acquitter pleinement de ses obligations».⁴⁷ Pour le moment, aucune date n'a encore été fixée pour la discussion en séance plénière au Parlement du projet de rapport. Les amendements de la Commission LIBE sauront-ils résister aux autres groupes politiques parlementaires et au Conseil?

Comparons à présent ce cadre interne au cadre offert par l'UE à ses citoyens lorsqu'elle coopère avec les Etats-Unis en matière de la lutte contre le financement du terrorisme, qui permet une identification encore plus nette des deux enjeux clés (droit à la protection des données et la sécurité) qui s'opposent dans notre problématique.

3. La mise en œuvre de la conception européenne de protection des données personnelles en matière pénale: perspective externe

Les attentats du 11 septembre ont accéléré la relance de la coopération sécuritaire, qui avait connu un ralentissement à la fin de la Guerre Froide. Une multitude d'accords bilatéraux et multilatéraux seront signés régissant la CPJP entre les Etats-Unis et l'UE⁴⁸ et des instruments spécifiques à la lutte anti-terroriste vont être mis en place, non sans conséquence pour la protection des données personnelles des citoyens européens.⁴⁹ L'impératif de sécurité nationale suppose que des mesures extraordinaires soient adoptées et rend légitimes de nombreux sacrifices à la protection de données.

L'accord TFTP (programme de surveillance du financement du terrorisme) relève de cette vague d'accords ciblant un aspect spécifique du terrorisme. Il a pour objectif de

⁴⁷ PE501.928v02-00, *op. cit.*, p. 111.

⁴⁸ De Busser, *op. cit.*, p. 26.

⁴⁹ *Ibid.*, p. 27.

prévenir, d'enquêter et de détecter les activités de financement du terrorisme.⁵⁰ Pour ce faire, SWIFT, organisme financier belge, transfère au Département Américain du Trésor des informations relatives aux transactions financières traitées⁵¹ afin que les Etats-Unis effectuent des croisements entre des transactions financières et des individus suspectés de financement du terrorisme. Ce transfert, qui est resté secret entre 2001 et 2006 a été révélé par deux journaux américains et vivement critiqué par le Parlement européen.⁵²

SWIFT a décidé par la suite de rapatrier en Europe ses activités, auparavant effectuées sur le sol américain. Or pour que l'échange d'informations puisse continuer, un accord entre l'UE et les Etats-Unis devait être conclu. Cet accord «SWIFT I» marque le début d'un long processus de négociation entre l'UE et les Etats-Unis, au cours duquel la protection des données personnelles occupera une place centrale.

3.1 La protection des données personnelles aux Etats-Unis: aux antipodes de la conception européenne?

Une fois que les données des citoyens européens parviennent sur le sol américain, elles sont traitées selon la législation américaine pour la protection des données. Cet échange d'informations doit donc être accompagné de règles communes relatives à la protection des données car bien que les définitions des données personnelles et du respect de la vie privée aux Etats-Unis et au sein de l'Union contiennent les mêmes éléments,⁵³ la protection des données aux Etats-Unis n'est pas inspirée d'une conception générale et chaque secteur est

⁵⁰ Union européenne, Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, JO L 195 du 27 Juillet 2010.

⁵¹ De Busser, *op. cit.*, p. 385.

⁵² Parlement européen, Résolution du 14 février 2007 sur SWIFT, l'accord PNR et le dialogue transatlantique sur ces questions, P7_TA(2007)0039, Strasbourg, JO C 287 du 29 novembre 2007; Résolution du 6 juillet 2006 sur l'interception des données des virements bancaires du système SWIFT par les services secrets américains, P6_TA(2006)0602, Strasbourg, JO C 303 du 13 décembre 2006.

⁵³ De Busser, *op. cit.*, p. 294.

réglementé par des règles de protection des données qui lui sont propres.⁵⁴ Ainsi, aucune réglementation particulière n'est prévue pour le domaine pénal.

Par ailleurs, les principes concrets de la protection des données personnelles diffèrent. Aux Etats-Unis, le texte de référence pour la protection des données personnelles est le *Privacy Act* de 1974, qui régit la protection des données en général. Ce dernier pose trois problèmes au regard de la coopération transatlantique.⁵⁵

Tout d'abord, il ne protège que les citoyens américains, car il s'applique aux «individus», qui sont définis comme tout «citoyen des Etats-Unis ou un étranger légalement admis pour une résidence permanente».⁵⁶ Par ailleurs, aucune base juridique n'a été établie pour le principe de finalité reconnu par le *Privacy Act*⁵⁷ et de nombreuses dérogations à ce principe sont possibles. Même si le consentement de la personne concernée n'est pas obtenu, les données peuvent être utilisées à des fins différentes que celles pour lesquelles elles avaient été collectées.⁵⁸ Alors que ce principe est considéré comme fondamental dans la conception européenne, il ne fait pas l'objet d'une affirmation suffisamment claire dans la loi américaine. Enfin, aucun principe général n'existe aux Etats-Unis pour la durée de conservation des données.⁵⁹ La signature de l'accord TFTP en 2010 va-t-elle permettre d'annihiler ces lacunes?

3.2 La conception européenne de protection des données dans l'accord TFTP: une difficile intégration

Si cet accord a été jugé indispensable par les autorités européennes et américaines pour éviter une nouvelle catastrophe, il n'est pas sans conséquences pour les données personnelles des citoyens européens. Ce lien nous permet d'étudier la mise en œuvre par l'UE de sa conception de la protection des données personnelles lors de ces négociations avec les Etats-Unis, et de déterminer la nature de cette mise en œuvre (totale ou partielle).

⁵⁴ *Ibid.*, p. 296.

⁵⁵ Bellanova et De Hert, *op. cit.*, p. 77.

⁵⁶ *Ibid.*, p. 74, voir §552 a(a)2, *Privacy Act* de 1974.

⁵⁷ Bellanova et De Hert, *loc. cit.*

⁵⁸ De Busser, *op. cit.*, p. 299.

⁵⁹ *Ibid.*, p. 302.

Pour étudier cette question, il faut tout d'abord rappeler les modifications apportées à l'accord entre ses versions de novembre 2009 et de juillet 2010 (SWIFT II) qui ont permis d'obtenir l'aval Parlement européen (qui avait préalablement rejeté le texte en février 2010).⁶⁰

L'accord prévoit la création d'un TFTP interne à l'UE, qui lui permettrait de mener elle-même ses propres enquêtes, et de n'envoyer aux Etats-Unis que les données relatives à une piste terroriste précise.⁶¹ Les principes de finalité et de nécessité sont également renforcés car SWIFT II prévoit qu'Europol devra étudier les requêtes américaines transmises à l'UE pour vérifier qu'elles répondent aux clauses de protection des données personnelles de l'accord, notamment la finalité et la nécessité.⁶² Enfin, SWIFT II prévoit que la loi américaine contienne des provisions sur les droits de la personne concernée.⁶³ L'action du Parlement européen a donc clairement permis de rétablir un certain équilibre entre la lutte contre le financement du terrorisme et la protection des données personnelles. Enfin, d'après le deuxième rapport de réexamen de l'application du TFTP présenté par la Commission européenne en décembre 2012, les garanties que prévoit l'accord ont été correctement mises en place.⁶⁴

Néanmoins, un groupe de députés de la Gauche Unitaire Européenne/Gauche Verte Nordique, et des Verts/Alliance Libre Européenne explique que «cet accord représente une violation claire de la législation communautaire sur la protection des données».⁶⁵ Certains commentateurs ont expliqué que le premier rejet de l'accord se fondait plus sur la volonté

⁶⁰ Parlement européen, Résolution législative du Parlement européen du 11 février 2010 sur la proposition de décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, P7_TA(2010)0029, Strasbourg, JO C 341 du 16 décembre 2010.

⁶¹ «EU to launch anti-terror finance tracking plan», Euractiv, 25 Mars 2010, consulté le 24 avril, <http://www.euractiv.com/financial-services/eu-launch-anti-terror-finance-tracking-plan-news-376447>.

⁶² Accord TFTP, article 4(2), *op. cit.*

⁶³ *Ibid.*, Article 18.

⁶⁴ Commission européenne, «Surveillance du financement du terrorisme: les garanties sont en place pour les citoyens», Communiqué de presse du 14 décembre 2012, IP/12/1366.

⁶⁵ Parlement européen, «SWIFT II: la commission des libertés approuve le projet d'accord», Communiqué de presse du 5 juillet 2010.

d'envoyer un signal politique clair au Conseil et à la Commission,⁶⁶ plutôt que sur une volonté de rétablir des standards de protection des données personnelles satisfaisants. Si cet argument peut en partie expliquer le comportement du Parlement dans «l'affaire SWIFT», il ne saurait délégitimer les critiques relatives aux données personnelles, que le CEPD ainsi que le Conseil Joint de Surveillance (CJS) ont également relevé.

Le CEPD a exprimé des doutes sur le respect du principe de proportionnalité, qui serait dénaturé selon lui par l'autorisation du transfert en masse des données, qui ne sera interdit qu'à long terme.⁶⁷ Le CJS estime que les requêtes américaines, qui ne sont transmises qu'oralement, et ne contiennent pas suffisamment de détails, ne permettent pas à Europol d'apprécier le respect ou la violation des principes de proportionnalité et de finalité, et ne lui permet donc pas de déterminer s'il doit accepter ou non la requête des autorités américaines.⁶⁸

Ces critiques sont également partagées par les eurodéputés Sophie In't Velt et Alexander Alvaro, qui estiment que le rapport du CJS devrait alerter la Commission car il prouve clairement qu'Europol ne remplit pas sa mission de garant de la protection des données.⁶⁹ Rapporteur du Parlement pour l'accord TFTP, Alexander Alvaro a même déclaré «à la lecture de ce rapport, les membres du Parlement européen se sentent trahis».⁷⁰

⁶⁶ Ambassade de France en Allemagne, «Revue de presse allemande», semaine du 5 au 12 février 2010, p. 2, consulté le 27 avril, http://www.botschaft-frankreich.de/IMG/pdf_20100212.pdf

⁶⁷ M. Cremona, *Justice and Home Affairs in a Globalised World: Ambitions and Reality in the tale of the EU-US SWIFT Agreement*, Institute for European Integration Research, Working Paper n° 4, Mars 2011, p. 20.

⁶⁸ *Report on the inspection of Europol's implementation of the TFTP agreement*, conduit en novembre 2010 par le Conseil Joint de Surveillance, Report n°JSB/INS.11-07, Bruxelles, 1 mars 2011, p. 5.

⁶⁹ «Terrorist Finance Tracking Programme is not respecting data protection safeguards», ALDE, Communiqué de presse, 5 mars 2011, consulté le 25 avril 2012, <http://www.alde.eu/press/press-and-release-news/press-release/article/terrorist-finance-tracking-programme-is-not-respecting-data-protection-safeguards-37202/>

⁷⁰ Parlement européen, «Rapport d'exécution SWIFT: importantes préoccupations en matière de protection des données», 13 mars 2011, consulté le 24 avril 2012, <http://www.europarl.europa.eu/news/fr/pressroom/content/20110314IPR15463/html/Un-rapport-d'exécution-SWIFT-sincèrement-préoccupant>.

3.3 Les pistes explicatives de ce décalage

Différentes hypothèses peuvent être formulées pour expliquer que l'UE ne soit pas totalement parvenue à «exporter» ses standards en matière de protection des données personnelles l'accord TFTP. D'une part, les relations diplomatiques entre les deux entités ne doivent en aucun cas être endommagées. Ainsi, à toutes les étapes de la négociation, l'UE s'est efforcée de maintenir le niveau de confiance établi, sans lequel aucun accord n'aurait jamais vu le jour.

On aurait pu en effet penser que compte tenu de l'enjeu d'un tel accord, l'UE était prête à coopérer à n'importe quel prix. L'accord signé avec les Etats-Unis n'étant pas réciproque, il ne profite qu'aux Etats-Unis, ce qui alimente la vision d'une UE minorisée dans les négociations. Cette perception doit être contrebalancée car le TFTP sert également les intérêts de l'UE: il lui permet de faire l'économie de l'extraction des données,⁷¹ et il a également permis d'empêcher certaines menaces terroristes de se concrétiser, grâce aux informations envoyées aux autorités policières des Etats membres.

Par ailleurs, si la Commission n'est pas parvenue à assurer pleinement la protection des données de ses citoyens, cela tient peut être au fait qu'elle ne connaissait pas les limites des sacrifices pouvant être faits à cette protection, car la conception européenne de protection des données en matière pénale ne fournit aucune indication sur les dérogations qui sont acceptables.

On aurait également pu faire l'hypothèse que les discussions intra-européennes relatives à l'approche globale auraient pu jouer un rôle dans ces négociations. La Commission avait lancé dès 2010 des discussions pour élever le niveau de protection des données, ce qui aurait pu «tirer vers le haut» les garanties de l'accord TFTP. Cependant la première communication de la Commission relative à cette approche globale date du 4 novembre 2010. Or l'accord TFTP a été conclu en juillet 2010. Si ces réflexions sur la

⁷¹ Entretien avec Cécilia Verkleij, Commission européenne, DG Home, Bruxelles, 28 mars 2012.

nouvelle approche se trouvaient bien dans les tuyaux des institutions, il est peu probable qu'elles aient eu une influence sur le TFTP.⁷²

Enfin, l'UE peut-elle se permettre «d'exporter et d'imposer» ses standards aux Etats-Unis? L'UE ne pouvait pas arriver à la table des négociations avec des revendications si fermes car les Etats-Unis auraient pris cette attitude comme une imposition. Si dès le départ, chaque partie avait entendu et compris les revendications et attentes de chacun, un juste-milieu devait être trouvé entre la vision européenne et la vision américaine de la protection des données. Ainsi, la perception d'une négociation déséquilibrée, au profit des Etats-Unis, durant laquelle l'UE aurait été *norm taker* peut donc être relativisée.

Cet accord a au moins le mérite de réguler la situation antérieure et certes, si dans l'accord, tous les standards européens de protection des données ne sont pas clairement établis, l'essentiel de cette conception y est intégré.

3.4 Les conséquences annexes de l'accord: favorables à la protection des données personnelles?

Sortons à présent de la vision classique associée à cet accord, et étudions deux phénomènes qui ont eu des conséquences positives pour la protection des données. D'une part, l'article 11 de cet accord prévoit qu'à terme, la Commission étudie «l'éventuelle introduction d'un système propre à l'Union européenne permettant un transfert plus ciblé de données».⁷³ Cet article a constitué la pré-condition au consentement du Parlement européen de la signature de l'accord. On peut se demander si cette clause n'est-elle pas purement symbolique, et uniquement destinée à obtenir l'aval du Parlement européen?

Les nombreux obstacles associés à la mise en place d'un tel système alimentent cette perception. Cela signifierait un coût supplémentaire pour l'UE, estimé par la Commission «entre €3 et €7 millions au démarrage, un montant supplémentaire de €7 à €11 millions

⁷² *Ibid.*

⁷³ Accord TFTP, article 11, *op. cit.*

étant nécessaire pour couvrir les frais de fonctionnement annuels». ⁷⁴ Par ailleurs, seuls quatre ou cinq Etats membres sont réellement concernés par la menace terroriste. ⁷⁵ Enfin, il faudrait renégocier l'accord conclu en juillet 2010, pour reformuler les modalités de transferts de données.

Pour éviter toute frustration américaine, l'UE a déjà informé les autorités américaines que la Commission travaillait sur l'éventuelle création du Système européen de Surveillance du Financement du Terrorisme (SSFT). ⁷⁶ L'avancement de ce projet est pour le moment relativement limité. Une communication de la Commission a été publiée le 13 juillet 2011, ⁷⁷ dans laquelle les différentes options possibles pour la mise en place du système sont exposées. Une analyse d'impact suivra cette communication avant que toute proposition de la Commission ne soit élaborée. ⁷⁸ Cependant, d'après un membre du Secrétariat du Conseil, la Commission européenne semble de plus en plus hésitante à poursuivre le projet, notamment au regard des coûts techniques et logistiques de la mise en place d'un tel système. Lors de la présentation du deuxième rapport de réexamen de l'application du TFTP présenté par la Commission européenne en décembre 2012, cette dernière a confirmé qu'une étude d'impact était actuellement en cours. ⁷⁹

Si un tel système était créé, cela permettrait à l'UE de ne transférer aux Etats-Unis que les données relatives aux individus pour lesquels un doute sérieux existe. ⁸⁰ Ainsi, l'extraction des données respecterait les principes de proportionnalité et de nécessité, ainsi que la Charte des droits fondamentaux. ⁸¹

⁷⁴ Commission européenne, Communication de la Commission au Parlement européen et au Conseil, Options envisageables pour la création d'un système européen de surveillance du financement du terrorisme, COM(2011) 429 final, Bruxelles, le 13 juillet 2011, p. 7.

⁷⁵ Entretien avec C.Verkleij, *op. cit.*

⁷⁶ *Ibid.*

⁷⁷ COM(2011) 429 final, *op. cit.*

⁷⁸ *Ibid.*

⁷⁹ Conseil de l'Union européenne, *Summary record of the meeting of the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE)*, 20 décembre 2012, Bruxelles, p. 9.

⁸⁰ «Mieux protéger les citoyens de l'UE : à l'image des Etats-Unis, créer un système européen de surveillance du financement du terrorisme. Un débat qui tombe à point!», EU logos, 17 juillet 2011, consulté le 27 avril 2012, http://www.eu-logos.org/eu-logos_nea-say.php?idr=4&idnl=2190&nea=111&lang=fra&lst=0

⁸¹ COM(2011) 429 final, *op. cit.*, p. 3.

D'autre part, afin d'éviter cette «dispute» récurrente à propos des données personnelles, l'UE et les Etats-Unis ont entamé dès 2006 un dialogue sur la faisabilité d'un accord pour la protection des données personnelles en matière pénale, au sein du *High Level Contact Group* (HLCG), afin d'aboutir à une convergence entre conceptions européenne et américaine de la protection des données en matière pénale.⁸² D'après les dernières informations disponibles, un mandat a été confié à la Commission par le Conseil pour négocier un accord-cadre, qui aurait pour but de produire un cadre légal que les transferts devraient respecter.⁸³

Cependant, d'après un membre du Conseil ayant participé à certaines réunions du HLCG, les négociations peinent à avancer, car les américains ont peur qu'un tel accord ne freine la coopération en matière pénale.⁸⁴ On pourrait alors penser que si un tel accord voyait le jour, sa portée serait largement affaiblie, pour ne pas «apeurer les Etats-Unis». Jusqu'ici, aucun accord n'a abouti à ce que la CPJP entre les Etats-Unis et l'UE ne soit entravée par des règles relatives à la protection des données. On sait déjà que les Etats-Unis ne sont pas prêts à modifier leur législation relative à la protection des données, et n'accepteront pas de voter un accord dit *legally binding*. Ils souhaitent un *executive agreement*, qui ne doit pas être ratifié par le Congrès et qui ne peut de ce fait aboutir à une modification de la législation américaine.⁸⁵ Un tel accord permettrait néanmoins de temporiser les discussions entre l'UE et les Etats-Unis pour la coopération pénale en général.

Ainsi, compte tenu de l'objet de l'accord (lutte contre le terrorisme) et de la nature même du partenaire américain, il est possible que les garanties dont les citoyens européens bénéficient dans cet accord ne soient pas totalement en adéquation avec la conception que l'UE applique entre ses Etats membres. Cependant, une telle vision doit être nuancée car des

⁸² Conseil de l'Union européenne, Final report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection, 15851/09, Bruxelles, 23 novembre 2009, p. 2.

⁸³ Conseil de l'Union européenne, «Communiqué de presse, 3050^{ème} session du Conseil Justice et Affaires Intérieures», 16918/10, 2 et 3 décembre 2010, Bruxelles, p. 27.

⁸⁴ Entretien avec un Haut Fonctionnaire, Secrétariat du Conseil de l'UE, *op. cit.*

⁸⁵ Entretien C.Verkleij, *op. cit.*, confirmé par l'entretien avec le Haut Fonctionnaire du Secrétariat du Conseil, *op. cit.*

changements ont été apportés à l'accord entre 2009 et 2010, et car les discussions sur le SSFT et sur l'accord bilatéral sur la protection des données en matière pénale n'auraient probablement jamais été envisagées sans les débats relatifs au TFTP.

Conclusion

Confrontés au choc sécuritaire post-11 septembre, les Etats membres de l'UE ont renforcé les lois sécuritaires et la coopération anti-terroriste avec les Etats-Unis a connu un regain. L'UE a donc été contrainte de réagir pour empêcher un usage incontrôlé des données personnelles des citoyens européens. Cette étude nous permet de conclure que lorsque l'UE réglemente la CPJP entre ses Etats membres, elle rencontre moins de difficulté à mettre en œuvre sa conception de la protection des données personnelles que lorsqu'elle coopère avec les Etats-Unis dans la lutte contre le financement du terrorisme.

Cela ne démontre pour autant pas un manque de cohérence de l'action de l'UE, car la transposition de la décision-cadre affaiblit la protection des données personnelles et car la coopération avec les Etats-Unis ne se fait pas systématiquement au détriment de la protection des données personnelles (voir les deux développements annexes à la signature de l'accord susmentionnés).

Si la réforme lancée en janvier 2012 n'a pas eu d'impact direct sur le TFTP, la dimension interne au sens large a permis que des garanties de protection des données personnelles soient intégrées dans l'accord. De même, si l'accord TFTP n'a pas eu de conséquences directes sur les débats relatifs à la réforme, il a conduit à envisager deux outils protecteurs des données personnelles. Cette réforme promet des garanties supplémentaires pour la protection des données personnelles, mais la poursuite du processus décisionnel pourrait dénaturer la proposition de la Commission. Par ailleurs, la coopération avec les Etats-Unis en matière pénale soulèvera toujours la problématique des données personnelles.

Le sujet est donc loin d'être épuisé, et l'avenir du traitement des données en matière pénale est relativement incertain. Face aux pressions sécuritaires, l'UE parviendra-t-elle à maintenir le cap de l'équilibre entre sécurité publique et protection des données personnelles? Ou sera-t-elle contrainte de sacrifier ce droit fondamental pour lutter contre les nouvelles menaces qui mettent en danger ses cinq cent millions citoyens?

Bibliographie

Alonso Blas, Diana, « First pillar and third pillar : need for a common approach on data protection ? » in *Reinventing Data Protection*, Gutwirth, Serge, Pouillet, Yves, De Hert, Paul (dir.), 2011, Dodrecht : Springer, pp. 225-237

Bellanova, Rocco et De Hert, Paul, *Protection des données personnelles et mesure de sécurité : vers une perspective transatlantique*, Cultures et Conflits, n° 74, été 2009, pp. 63-80

Coudray, Ludovic, *La protection des données personnelles dans l'Union européenne, Naissance et consécration d'un droit fondamental*, Editions universitaires européennes, Editions universitaires européennes, Saarbruck, 2010, pp. 243-630

Cremona, Marise, *Justice and Home Affairs in a Globalised World: Ambitions and Reality in the tale of the EU-US SWIFT Agreement*, Institute for European Integration Research, Working Paper n° 4, Mars 2011, pp. 1-30

De Busser, Els, *Data protection in EU and US criminal cooperation, A substantive law approach to the EU internal and transatlantic cooperation in criminal matters between judicial and law enforcement authorities*, Maklu Publishers, 2009, pp. 84-123 et pp. 219-423

De Busser, Els, *EU data protection in transatlantic cooperation in criminal matters : Will the EU be serving its citizens an American meal?*, Utrecht Law Review, Volume 6, Issue 1, 2010, pp. 86-100

Deffains, Nathalie, *Traitement de données à caractère personnel et droit au respect de la vie privée devant la Cour européenne des droits de l'homme*, Techniques et droit humain, Actes du Colloque organisé du 20 au 23 avril 2010, Montchrestien 2011, pp. 253-270

Pfisterer, Valentin, *The Second SWIFT Agreement Between the European Union and the United States of America – An Overview*, German Law Journal, Vol 11 n° 10, 1 October 2010, 1173-1190

Rodota, Stefano, « Data protection as a fundamental right », dans *Reinventing Data Protection ?*, Gutwirth, Serge, Poullet, Yves, De Hert, Paul, (dir.), 2011, Dodrecht : Springer, pp. 78-82

Türk, Axel, Piazza, Pierre, *La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée*, Cultures et Conflits, Fichage et Listing, n°76, hiver 2009, pp. 114-133

Documents officiels

- Commission européenne

Commission des Communautés européennes, *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*, COM(2005) 475 final, Bruxelles, 4 octobre 2005, pp. 2-6

Commission européenne, *Communication de la Commission au Parlement européen et au Conseil, Options envisageables pour la création d'un système européen de surveillance du financement du terrorisme*, COM(2011) 429 final, Bruxelles, 13 juillet 2011

Commission européenne, *Communication de la Commission : Protection de la vie privée dans un monde en réseau, Un cadre européen relatif à la protection des données, adapté aux défis du 21^{ème} siècle*, COM(2012) 9 final, Bruxelles, 25 Janvier 2012

Commission européenne, *Proposition de directive du Parlement européen et du Conseil, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données*, 2012 COM(2012) 10 final, Bruxelles, 25 janvier 2012, pp. 1-17

Commission européenne, *Rapport de la Commission fondé sur l'article 29, paragraphe 2, de la décision-cadre du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale*, COM(2012) 012 final, 25 janvier 2012, JO C102/38 du 5 avril 2012, pp. 1-6

- Conseil de l'Union européenne

Conseil de l'Union européenne, *Décision-cadre (2008/977/JAI) du 27 novembre 2008, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale*, JO L 350 du 30 décembre 2008

Conseil de l'Union européenne, *Final report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection*, 15851/09, Bruxelles, 23 novembre 2009

Conseil de l'Union européenne, « Communiqué de presse, 3050^{ème} session du Conseil Justice et Affaires Intérieures », 16918/10, Bruxelles, 2 et 3 décembre 2010

- Conseil de l'UE et Parlement européen

Parlement Européen et Conseil, *Directive (95/46/CE) 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 novembre 1995

- Parlement européen

Parlement européen, *Rapport sur le premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE)*, Marco Cappato, 24 février 2004, pp. 1-10

Parlement européen, *Rapport contenant une proposition de recommandation du Parlement européen à l'intention du Conseil sur l'évolution des négociations sur la décision-cadre sur la protection des données dans le cadre de la coopération policière et judiciaire en matière pénale*, P6_TA(2006)0602, Strasbourg, 14 décembre 2006

Parlement européen, *Résolution du 14 février 2007 sur SWIFT, l'accord PNR et le dialogue transatlantique sur ces questions*, P6_TA(2007)0039, Strasbourg, JO C 287 du 29 novembre 2007

Parlement européen, Résolution législative du Parlement européen du 11 février 2010 sur la proposition de décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, P7_TA(2010)0029, JO C 341 du 16 décembre 2010

Parlement européen, « Rapport d'exécution SWIFT : importantes préoccupations en matière de protection des données », 13 mars 2011, consulté le 24 avril 2012, <http://www.europarl.europa.eu/news/fr/pressroom/content/20110314IPR15463/html/Un-rapport-d'exécution-SWIFT-sincèrement-préoccupant>

- Conseil de l'Europe

Conseil de l'Europe, *Convention européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales*, Série des traités du Conseil de l'Europe n° 005, Rome, 4 novembre 1950

Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, 28 Janvier 1981, Série des traités européens, n° 108

Conseil de l'Europe, *Recommandation n° 87 (15), du Comité des Ministres aux Etats Membres, Visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police*, 17 septembre 1987, lors de la 410^{ème} réunion des Délégués des Ministres

- Contrôleur Européen de la Protection des Données

CEPD, *Avis du contrôleur européen de la protection des données du 19 décembre 2005 sur la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité*, JO C47 du 25 février 2006

CEPD, *Avis du 29 novembre 2006 Second opinion of the European Data Protection Supervisor of the 29 November 2006 on the proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, JO C91 du 26 avril 2007

CEPD, *Avis Troisième avis du contrôleur européen de la protection des données du 27 avril 2007 sur la 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*, JO C139, du 23 juin 2007

Hustinx, Peter, Newsletter du CEPD, n°31, 28 janvier 2012

- Autres

Union européenne, *Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme*, JO L 195 du 27 Juillet 2010

Davoli, Alessandro, *La protection des données à caractère personnel*, Parlement européen, Fiche technique 4.12.8, mars 2011

Report on the inspection of Europol's implementation of the TFTP agreement, conduit en novembre 2010 par le Conseil Joint de Surveillance, Report n°JSB/INS.11-07, Bruxelles, 1 mars 2011

Déclaration 21 annexée à l'acte final de la Conférence intergouvernementale qui a adopté le Traité de Lisbonne, signé le 13 décembre 2007, JO C 83 du 30 mars 2010

Articles internet

« Mieux protéger les citoyens de l'UE : à l'image des Etats-Unis, créer un système européen de surveillance du financement du terrorisme. Un débat qui tombe à point ! », *EU logos*, 17 juillet 2011, consulté le 27 avril 2012, http://www.eu-logos.org/eu-logos_nea-say.php?idr=4&idnl=2190&nea=111&lang=fra&lst=0

« Update on a Council framework decision on the protection of personal data », *European Digital Rights*, 20 Juin 2007, consulté le 6 avril 2012, <http://www.edri.org/edriagram/number5.12/framework-decision-data-protection>

« EU to launch anti-terror finance tracking plan », *Euractiv*, 25 Mars 2010, consulté le 24 avril, <http://www.euractiv.com/financial-services/eu-launch-anti-terror-finance-tracking-plan-news-376447>

« Terrorist Finance Tracking Programme is not respecting data protection safeguards », *ALDE*, Communiqué de presse, 5 mars 2011, consulté le 25 avril 2012, <http://www.alde.eu/press/press-and-release-news/press-release/article/terrorist-finance-tracking-programme-is-not-respecting-data-protection-safeguards-37202/>

« SWIFT II: la commission des libertés approuve le projet d'accord », Parlement européen, Communiqué de presse du 5 juillet 2010

Ambassade de France en Allemagne, « Revue de presse allemande », semaine du 5 au 12 février 2010, consulté le 27 avril, http://www.botschaft-frankreich.de/IMG/pdf_20100212.pdf

Entretiens

Haut Fonctionnaire, Secrétariat du Conseil, Entretien, DG H, Bruxelles, 11 avril 2012

Haut Fonctionnaire, DG Justice, Entretien, Commission européenne, Bruxelles, 7 mars 2012

Député européen, Parlement européen, Entretien, Comité LIBE, 28 mars 2012

Verkleij, Cécilia, Commission européenne, Entretien, DG Home, Bruxelles, 28 mars 2012

Bruges Political Research Papers / Cahiers de recherche politique de Bruges

No 28 / 2013

Marta Zalewska and Oskar Josef Gstrein, National Parliaments and their Role in European Integration: The EU's Democratic Deficit in Times of Economic Hardship and Political Insecurity

No 27 / 2012

Laura Batalla Adam, The Significance of EU Topics in National Media: Has There Been a Europeanization of Reporting in the National Media?

No 26 / 2012

Claire Baffert, Participatory Approaches In The Management Of Natura 2000: When EU Biodiversity Policy Gets Closer to its Citizens

No 25 / 2012

Serena Garelli, The European Union's Promotion of Regional Economic Integration in Southeast Asia: Norms, Markets or Both?

No 24 / 2012

Luis Bouza García, Víctor Cuesta López, Elitsa Mincheva and Dorota Szeligowska, The European Citizens' Initiative – A First Assessment

No 23 / 2012

Isabelle de Lichtervelde, La défense des droits de l'homme en Chine : Le parlement européen est-il la voix normative de l'union européenne ?

No 22 / 2012

Erik Brattberg and Mark Rhinard, The EU and US as International Actors in Disaster Relief

No 21 / 2011

Alesia Koush, Fight against the Illegal Antiquities Traffic in the EU: Bridging the Legislative Gaps

No 20 / 2011

Neill Nugent and Laurie Buonanno, Explaining the EU's Policy Portfolio: Applying a Federal Integration Approach to EU Codecision Policy

No 19 / 2011

Frederika Cruce, How Did We End Up with This Deal? Examining the Role of Environmental NGOs in EU Climate Policymaking

No 18 / 2011

Didier Reynders, Vers une nouvelle 'gouvernance économique'?

No 17 / 2010

Violeta Podagélytė, Democracy beyond the Rhetoric and the Emergence of the "EU Prince": The Case of EU-Ukraine Relations

No 16 / 2010

Maroš Šefčovič, From Institutional Consolidation to Policy Delivery

No 15 / 2010

Sven Biscop and Jo Coelmont, Permanent Structured Cooperation in Defence: Building Effective European Armed Forces

No 14 / 2010

Antonio Missiroli, Implementing the Lisbon Treaty: The External Policy Dimension

No 13 / 2010

Anne-Céline Didier, The European Institute of Innovation and Technology (EIT): A New Way for Promoting Innovation in Europe?

No 12 / 2010

Marion Salines, Success Factors of Macro-Regional Cooperation: The Example of the Baltic Sea Region

No 11 / 2010

Martin Caudron, Galileo: Le Partenariat Public-Privé à l'Épreuve du « Juste Retour »

No 10 / 2009

Davide Bradanini, The Rise of the Competitiveness Discourse—A Neo-Gramscian Analysis

No 9 / 2009

Adina Crisan, La Russie dans le nouveau Grand Jeu énergétique en Mer Noire: Nabucco et South Stream ou « l'art du kuzushi »

No 8 / 2008

Jonas Dreger, The Influence of Environmental NGOs on the Design of the Emissions Trading Scheme of the EU: An Application of the Advocacy Coalition Framework

No 7 / 2008

Thomas Kostera, Europeanizing Healthcare: Cross-border Patient Mobility and Its Consequences for the German and Danish Healthcare Systems

06 / 2007

Mathieu Rousselin, Le Multilatéralisme en Question : Le Programme de Doha pour le Développement et la Crise du Système Commercial Multilatéral

05 / 2007

Filip Engel, Analyzing Policy Learning in European Union Policy Formulation: The Advocacy Coalition Framework Meets New-Institutional Theory

04 / 2007

Michele Chang, Eric De Souza, Sieglinde Gstöhl, and Dominik Hanf, Papers prepared for the Colloquium, “Working for Europe: Perspectives on the EU 50 Years after the Treaties of Rome”

03 / 2007

Erwin van Veen, The Valuable Tool of Sovereignty: Its Use in Situations of Competition and Interdependence

02 / 2007

Mark Pollack, Principal-Agent Analysis and International Delegation: Red Herrings, Theoretical Clarifications, and Empirical Disputes

01 / 2006

Christopher Reynolds, All Together Now? The Governance of Military Capability Reform in the ESDP



Europe is in a constant state of flux. European politics, economics, law and indeed European societies are changing rapidly. The European Union itself is in a continuous situation of adaptation. New challenges and new requirements arise continually, both internally and externally.

The *College of Europe Studies* series seeks to publish research on these issues done at the College of Europe, both at its Bruges and its Natolin (Warsaw) campus. Focused on the European Union and the European integration process, this research may be specialised in the areas of political science, law or economics, but much of it is of an interdisciplinary nature. The objective is to promote understanding of the issues concerned and to make a contribution to ongoing discussions.

L'Europe subit des mutations permanentes. La vie politique, l'économie, le droit, mais également les sociétés européennes, changent rapidement. L'Union européenne s'inscrit dès lors dans un processus d'adaptation constant. Des défis et des nouvelles demandes surviennent sans cesse, provenant à la fois de l'intérieur et de l'extérieur.

La collection des *Cahiers du Collège d'Europe* publie les résultats des recherches menées sur ces thèmes au Collège d'Europe, au sein de ses deux campus (Bruges et Varsovie). Focalisés sur l'Union européenne et le processus d'intégration, ces travaux peuvent être spécialisés dans les domaines des sciences politiques, du droit ou de l'économie, mais ils sont le plus souvent de nature interdisciplinaire. La collection vise à approfondir la compréhension de ces questions complexes et contribue ainsi au débat européen

Series Titles:

- vol. 16** Chang, Michele / Monar, Jörg (eds.), *The European Commission in the Post-Lisbon Era of Crises: Between Political Leadership and Policy Management*, 2013 (298 p.), ISBN 978-2-87574-028-1 pb.
- vol. 15** Mahnke, Dieter / Gstöhl, Sieglinde (eds.), *European Union Diplomacy: Coherence, Unity and Effectiveness*, 2012 (273 p.) ISBN 978-90-5201-842-3 pb.
- vol. 14** Lannon, Erwan (ed.), *The European Neighborhood Policy's Challenges*, 2012 (491p.), ISBN 978-90-5201-779-2 pb.
- vol. 13** Cremona, Marise / Monar, Jörg / Poli Sara (eds.), *The External Dimension of the European Union's Area of Freedom, Security and Justice*, 2011 (432 p.), ISBN 978-90-5201-728-0 pb.
- vol. 12** Men, Jong / Balducci, Giuseppe (eds.), *Prospects and Challenges for EU-China Relations in the 21st Century*, 2010 (262 p.), ISBN 978-90-5201-641-2 pb.
- vol. 11** Monar, Jörg (ed.), *The Institutional Dimension of the European Union's Area of Freedom, Security and Justice*, 2010 (268 p.), ISBN 978-90-5201-615-3 pb.
- vol. 10** Hanf, Dominik / Malacek, Klaus / Muir, elise (eds.), *Langues et construction européenne*, 2010 (286 p.), ISBN 978-90-5201-594-1 pb.
- vol. 9** Pelkmans, Jacques / Hanf, Dominik / Chang, Michele (eds.), *The EU Internal Market in Comparative Perspective*, 2008 (314 p.), ISBN 978-90-5201-424-1 pb.
- vol. 8** Govaere, Inge / Ullrich, Hanns (eds.), *Intellectual Property, Market Power and the Public Interest*, 2008 (315 p.), ISBN 978-90-5201-422-7 pb.
- vol. 7** Inotai, András, *The European Union and Southeastern Europe: Troubled Waters Ahead?*, 2007 (414 p.), ISBN 978-90-5201-071-7 pb.
- vol. 6** Govaere, Inge / Ullrich, Hanns (eds.), *Intellectual Property, Public Policy, and International Trade*, 2007 (232 p.), ISBN 978-90-5201-064-9 pb.
- vol. 5** Hanf, Dominik / Muñoz, Rodolphe (eds.), *La libre circulation des personnes: États des lieux et perspectives*, 2007 (329 p.), ISBN 978-90-5201-061-8 pb.
- vol. 4** Mahncke, Dieter / Gstöhl, Sieglinde (eds.), *Europe's Near Abroad: Promises and Prospects of the EU's Neighbourhood Policy*, 2008 (316 p.), ISBN 978-90-5201-047-2.
- vol. 3** Mahncke, Dieter / Monar, Jörg (eds.), *International Terrorism: A European Response to a Global Threat?* 2006 (191p.), ISBN 978-90-5201-046-5 / US-ISBN 978-0-8204-6691-0 pb.
- vol. 2** Demaret, Paul / Govaere, Inge / Hanf, Dominik (eds.), *European Legal Dynamics - Dynamiques juridiques européennes*, Revised and updated edition of *30 Years of European Legal Studies at the College of Europe*, 2005 / 2007 (571 p.), ISBN 978-90-5201-067-0 pb.
- vol. 1** Mahncke, Dieter / Ambos, Alicia / Reynolds, Christopher (eds.), *European Foreign Policy: From Rhetoric to Reality?*, 2004 / second printing 2006 (381 p.), ISBN 978-90-5201-247-6 / US-ISBN 978-0-8204-6627-9 pb.

If you would like to be added to the mailing list and be informed of new publications and department events, please email rina.balbaert@coleurope.eu. Or find us on Facebook: College of Europe Politics and Administration Department.