L'Union européenne et les technologies de sécurité

Sylvia Preuss-Laussinotte

Édition électronique

URL : <http://journals.openedition.org/conflits/2142>

DOI : 10.4000/conflits.2142

ISSN : 1777-5345

Éditeur :

CCLS - Centre d'études sur les conflits liberté et sécurité, L'Harmattan

Édition imprimée

Date de publication : 20 décembre 2006

Pagination : 97-108

ISBN : 978-2-296-02667-4

ISSN : 1157-996X

Référence électronique

Sylvia Preuss-Laussinotte, « L'Union européenne et les technologies de sécurité », *Cultures & Conflits* [En ligne], 64 | hiver 2006, mis en ligne le 06 mars 2007, consulté le 30 mars 2021. URL : <http://journals.openedition.org/conflits/2142> ; DOI : <https://doi.org/10.4000/conflits.2142>

Ce document a été généré automatiquement le 30 mars 2021.

Creative Commons License

L'Union européenne et les technologies de sécurité

Sylvia Preuss-Laussinotte

- 1 L'Union européenne a incontestablement joué – et joue encore – un rôle central dans le domaine des technologies de sécurité, devenant un véritable « moteur » pour ses Etats membres, notamment en matière de biométrie. Pour accompagner le recours à ces technologies, elle met en place depuis quelques années un cadre juridique qu'elle désigne comme devant être « cohérent ». Cet objectif de « cohérence juridique » rappelle celui de « convergence juridique », qui n'avait pourtant rencontré qu'un écho très mitigé lorsqu'il avait été proposé en 1997 : face au constat de la convergence inéluctable des technologies de l'information et de la communication, l'Union avait jugé nécessaire d'accompagner cette convergence par une restructuration juridique. Mais, lorsque la Commission européenne avait publié un Livre vert sur la convergence ¹ – et proposé un cadre juridique nouveau et commun pour l'ensemble des secteurs des nouvelles technologies –, les Etats avaient majoritairement opté pour le rejet de cette proposition et pour le maintien de leurs cadres juridiques, en acceptant quelques vagues aménagements. Si le terme « convergence » a été abandonné pour celui de « cohérence », heurtant moins les sensibilités étatiques, les questions posées restent pourtant les mêmes, liées à la difficulté de mettre en place une véritable politique commune en matière de sécurité. C'est à partir de ce constat que nous tenterons d'analyser, sous l'angle juridique, le rôle de l'Union européenne dans le recours aux technologies de sécurité, illustrant sa recherche plus générale d'unification dans le domaine des politiques de sécurité, qui ne dépendent plus du seul traité sur l'Union européenne – et donc de la seule politique pénale – depuis le transfert au traité de Rome des politiques d'asile, d'immigration, de visas et de contrôle aux frontières.

L'objectif de cohérence juridique en matière de technologies de sécurité

- 2 L'usage des technologies de sécurité en Europe s'est essentiellement traduit par le recours à la biométrie et aux bases de données, ces deux éléments étant indissociables. Ainsi, en quelques années, la biométrie a été appliquée à un ensemble de domaines : politique des visas et contrôle aux frontières liés à la gestion des flux migratoires,

prévention et répression de la criminalité, surveillance et prévention du danger extérieur / intérieur que représente le terrorisme, et ce, malgré la difficulté inhérente à la construction européenne. La « ventilation » entre ces domaines, selon qu'ils dépendent du premier pilier communautaire ou du troisième pilier « coopération policière et judiciaire pénale ² » reste complexe, l'objectif de « cohérence juridique » visant aussi à uniformiser ces domaines, malgré leur séparation juridique.

- 3 Dès 1998, le plan d'action de Vienne, adopté par le Conseil JAI du 3 décembre 1998, prévoit que l'évolution des moyens techniques doit être suivie attentivement, afin d'améliorer la sécurité du modèle type de visa mis en place en 1995 ³. Cette position est confirmée dans le cadre des conclusions du Conseil européen de Tampere des 15 et 16 octobre 1999, convenant de poursuivre la mise en place d'une politique commune active en matière de visas et de faux documents. Le Conseil européen de Thessalonique, les 19 et 20 juin 2003, va surtout insister sur la nécessité de dégager au sein de l'Union européenne une « approche cohérente » en ce qui concerne les identificateurs ou les données biométriques pour les documents des ressortissants de pays tiers, les passeports des citoyens de l'Union et les systèmes d'information qui vont intégrer ces données biométriques pour permettre l'authentification par comparaison (VIS et SIS II). Enfin, le « programme de La Haye », adopté par le Conseil européen le 5 novembre 2004, va prendre pour objectif l'approfondissement de cette approche commune, désormais à vingt-cinq Etats membres, et le traitement plus efficace des actions communes que sont la prévention (du terrorisme, de l'immigration illégale, de la criminalité) et la surveillance. Il est rappelé avec insistance que l'Union européenne doit adopter une « approche juridique cohérente et des solutions harmonisées » en matière d'identificateurs et de données biométriques.
- 4 Suivant une logique déjà à l'œuvre dans les Etats membres, la décision d'intégrer des éléments biométriques, à savoir la photographie du visage et les empreintes digitales, a d'abord été prise dans le cadre de la politique d'immigration européenne, en relation étroite avec la mise en place de bases de données destinées à assurer la comparaison de ces éléments biométriques aux fins d'authentification et de vérification ⁴. La Commission indique d'ailleurs – de façon révélatrice – que, dans le contexte de libre circulation des personnes dans l'UE, la dernière bases de données créée, le VIS ⁵ « représente une des grandes initiatives des politiques de l'UE destinées à favoriser la stabilité et la sécurité », le recours aux données biométriques étant présenté comme le gage de cette sécurité.
- 5 Pour accompagner cette évolution rapide des bases de données vers l'intégration de la biométrie, le Conseil européen de La Haye a demandé au Conseil de l'UE d'étudier les moyens « d'optimiser l'efficacité et l'interopérabilité des systèmes d'information de l'Union européenne » pour lutter contre l'immigration clandestine et améliorer les contrôles aux frontières, ainsi que la gestion de ces systèmes, en se fondant sur une communication de la Commission, relative à l'interopérabilité entre les systèmes ⁶, et « en tenant compte de la nécessité de trouver le juste milieu entre les objectifs répressifs et la préservation des droits fondamentaux des personnes ». Allant plus loin, la Commission a présenté une proposition illustrant le souhait qu'à terme, l'ensemble de ces fichiers soit interconnecté et ne forme plus qu'une seule immense base de données ⁷, prouvant sa volonté d'unification dans ce domaine.
- 6 Il est clair que l'objectif de « cohérence juridique » va dans le sens d'un accompagnement de la convergence technique des systèmes européens contenant des

données biométriques, pour des motifs dont l'aspect de « cohérence budgétaire » n'est pas absent. Cet objectif de cohérence vise également à favoriser les interconnexions entre bases de données nationales et européennes, notamment biométriques.

- 7 Il est intéressant de noter qu'en application de ces objectifs,

« sous l'impulsion de la Direction générale JLS (Justice Liberté et Sécurité), de grands programmes voient le jour et se dessinent. Ces programmes portent essentiellement aujourd'hui sur une gestion plus efficace des frontières de l'Union avec des projets comme BMS (Biometric Matching System), BIODIV (Biometric Data Experimented in Visas) par exemple ou encore l'annonce pour 2008 de passeports biométriques à empreintes digitales. Sur ce dernier point l'Europe, contrairement aux Etats-Unis, traitera de la même façon ses citoyens et ses visiteurs. En revanche, pour des raisons structurelles évidentes, l'Europe mettra probablement plus de temps à articuler les projets biométriques de gestion d'identité comparables aux programmes américains TWIC ou PIV ⁸ ».

Les contraintes extérieures

- 8 L'objectif de « cohérence » de l'Union européenne présenté comme nécessaire pour l'élaboration d'une politique européenne de sécurité apparaît toutefois quelque peu ambigu, notamment du fait des contraintes extérieures qui l'accompagnent, et ce, de manière désormais explicite depuis le 11 septembre 2001 : c'est au nom de la lutte contre le terrorisme et sous la pression sans appel des Etats-Unis que l'Europe va recourir à la biométrie et en faire l'un de ses objectifs prioritaires.

- 9 Le recours à la biométrie comme moyen de protection contre le terrorisme est évoqué dès 2002 dans le cadre d'un rapport de l'OTAN :

« Ces technologies pourraient également servir à l'émission de documents officiels (passeports, cartes d'accès, permis de conduire ou carte de sécurité sociale) dont beaucoup ont déjà été pourvus de minuscules puces électroniques comportant des données personnelles. Ces puces pourraient aussi contenir une version cryptée d'un identifiant biométrique spécifique, tel que la numérisation d'une empreinte digitale ou d'un iris. Cela rendrait toute falsification pratiquement impossible et empêcherait les substitutions d'identités. Cette même technologie pourrait s'appliquer aux visas accordés aux visiteurs étrangers ⁹ ».

- 10 Cette position, désormais adoptée par l'Union européenne, a pour origine la politique de l'Organisation internationale de l'aviation civile (OACI) en matière de documents de voyage, déjà ancienne mais longtemps restée non obligatoire. Les attentats du 11 septembre 2001, directement liés à l'aviation, ont permis de justifier très rapidement le recours à la biométrie pour ces documents. En juillet 2005, après les attentats de Londres – qui se sont, rappelons-le, déroulés dans le métro londonien et non dans un aéroport –, l'OACI a pris la décision immédiate de rendre obligatoire les données biométriques dans les documents de voyage ¹⁰. L'insertion d'éléments biométriques dans ce type de documents a donc été décidée en Europe, comme au niveau mondial, en fonction de normes communes issues des choix effectués dans le cadre de l'OACI ¹¹. En effet, les articles 22, 23 et 37 de la Convention de Chicago ¹² lient les Etats contractants dans le domaine de la définition et l'adoption des normes internationales pour les douanes, l'immigration et autres procédures, dans le but de faciliter les processus transfrontaliers qui interviennent dans le transport aérien international.

- 11 L'OACI, en relation directe avec l'Organisation internationale de normalisation (ISO), a donc clairement joué un rôle central dans la conception et la définition des normes biométriques applicables en Europe. Dans le contexte de l'après-11 septembre 2001, ces normes se sont imposées, la convention de Chicago obligeant les Etats à respecter les

normes édictées par l'OACI pour des raisons de sécurité des transports aériens. Or, ces normes sont définies de manière à assurer l'interopérabilité des systèmes de contrôle dans les aéroports des cent quatre-vingt-neuf Etats membres, notamment par l'utilisation d'un système de lecture optique standardisé des documents de voyage, désignés par l'OACI comme étant des MRTD (Machine Readable Travel Documents, documents de voyage lisibles à la machine). Selon la définition de l'OACI, les MRTD sont « des documents de voyage internationaux, tels que passeport ou visa, qui renferment des données lisibles à l'œil et à la machine ¹³ ». Les spécifications du groupe consultatif technique sont publiées dans le document 9303 de l'OACI, référence qui figure désormais explicitement dans les règlements européens sur les passeports ¹⁴, sur les titres de séjour ¹⁵, et sur les visas, où il est indiqué que le document « doit comporter des dispositifs de sécurité harmonisés, universellement reconnaissables » (photographie numérique et deux empreintes digitales selon les normes OACI décrites comme étant des normes techniques de haut niveau).

12 Or, selon les déclarations d'un représentant de l'OACI :

« Evidemment, [l'organisation] ne l'a pas fait uniquement pour l'aviation, ni dans un cadre isolé. Elle a collaboré avec d'autres organisations internationales comme Interpol et l'Organisation internationale du travail (OIT) en ce qui concerne les documents de voyage des marins ¹⁶ ».

13 Cet élément amène à émettre quelques réserves, voire des inquiétudes, face à l'optimisme technologique proclamé notamment au regard de cette utilisation mondiale d'éléments biométriques, aboutissant à la création de bases de données internationales et nationales interopérables, tous les Etats utilisant les mêmes normes OACI pour les documents de voyage qu'ils délivrent, en relation avec les techniques de visualisation, elles aussi prévues et normalisées dans le cadre de l'OACI. Comme l'a clairement indiqué un représentant de SAGEM, entreprise extrêmement présente dans le domaine de la biométrie et des documents d'identité : « L'usage de la biométrie, comme technologie permettant de gérer des grands flux aux frontières sans failles de sécurité, devient le ferment d'une biométrie mondiale interopérable ». Or, c'est précisément dans la mise en place de cette mondialisation biométrique généralisée que se pose la question de sa fragilité, et de celle de la politique européenne de sécurité.

14 Face à l'optimisme très actif des entreprises auxquelles ont recours l'Europe et les Etats, le groupe « Article 29 » avait fait part de ses extrêmes réserves concernant le recours à de telles données biométriques, rappelées dans un courrier du 30 novembre 2004. Contredisant l'argument de sécurisation des documents d'identité, le groupe souligne :

« des résultats d'essais ont toutefois montré que les procédés reposant sur des éléments biométriques ne garantissaient ni la sécurité requise ni la commodité escomptée pour les voyageurs, vu que le pourcentage d'acceptation erronée ou de rejet erroné du détenteur du passeport par le système de sécurité de reconnaissance semble élevé ».

15 Dans la même optique, le CEPD (Contrôleur européen à la protection des données), tout en approuvant l'harmonisation de la politique européenne d'immigration, en particulier avec un format uniforme de titre de séjour, rappelle que « celui-ci n'est pas un document de voyage, mais un document d'identité, et doit en conséquence bénéficier des mêmes standards de sécurité que les cartes d'identité nationales ¹⁷ ». Pour lui, « il n'existe aucune raison de suivre les standards de l'OACI, notamment le

recours aux puces sans contact » dont on connaît les risques de lecture à distance ¹⁸. Il s'agit là des rares critiques officielles à l'application des standards OACI.

- 16 La matérialisation de contraintes extérieures, pourtant incompatibles avec la philosophie européenne proclamée en matière de données personnelles, est illustrée par la position de l'UE face aux exigences américaines en matière de transfert des données passagers (PNR et API). Malgré l'inexistence connue d'une protection des données personnelles aux Etats-Unis ¹⁹, la Commission européenne a publié une décision d'adéquation à leur bénéfice ²⁰; cette décision avait pourtant fait l'objet de critiques sévères par le Groupe article 29 ²¹ et le Contrôleur européen à la protection des données (CEPD), qui est même intervenu au cours de la procédure intentée par le Parlement européen devant la CJCE. Cette gigantesque récolte de données personnelles n'aura pourtant aucun effet sur la prévention du terrorisme, malgré le discours officiel de justification. L'annulation, le 30 mai 2006 ²², pour de simples motifs de forme de cette décision et de l'accord entre l'Union européenne et les Etats-Unis sur le transfert des données PNR n'a pas entraîné trop de dégâts collatéraux : chaque Etat membre peut, de manière bilatérale, continuer à communiquer ces données.
- 17 Mais les institutions européennes ont signé dans la précipitation un nouvel accord ²³, en retrait par rapport au précédent, qui éclaire sous un jour qui n'est pas nouveau les raisons d'un tel processus : il n'est enfin plus caché que ces données personnelles PNR sont destinées aux agences de sécurité américaines s'occupant de la lutte contre le terrorisme et la criminalité, même s'il est demandé aux USA que le système ne soit pas doté d'un accès généralisé, mais d'un système « push » (approche au cas par cas), et « d'assurer une stricte limitation des objectifs, de sorte que les données relatives au comportement ne puissent être utilisées à des fins d'identification de délits financiers ou de prévention de la grippe aviaire ²⁴ ». Il ne fait pourtant guère de doute que la protection américaine des données personnelles n'a pas évolué. Les justifications avancées sont donc davantage de l'ordre de la précaution oratoire destinée à dédouaner les institutions européennes jouant sur le constat avoué que sans accord, le transfert de données se ferait de toutes façons, la menace de blocage des vols européens étant suffisante pour l'accepter. Selon cette position, mieux vaut un accord permettant un éventuel contrôle et garantissant une protection même restreinte des personnes. Or, la seule protection qui figure dans l'accord est la possibilité de « suspension de transfert » des données
- « lorsqu'il existe une forte probabilité que les normes de protection applicables ne sont pas respectées, qu'il y a des motifs raisonnables de croire que le DHS [ministère américain de la sécurité intérieure] ne prend pas ou ne prendra pas, en temps voulu les mesures adéquates qui s'imposent pour régler l'affaire en question, que la poursuite du transfert entraînerait un risque imminent de grave préjudice pour les personnes concernées et que les autorités compétentes de l'Etat membre concerné se sont raisonnablement efforcées, dans ces circonstances, d'avertir le DHS et de lui donner la possibilité de répondre ».
- 18 Cette position a une conséquence considérée comme positive, puisqu'elle permet à l'UE de disposer elle aussi d'un système PNR en élargissant le transfert de données à tous les vols en Europe, même si le Parlement a rejeté cette idée par trois fois. Le Parlement européen reconnaît pourtant clairement que l'objectif à long et moyen terme de ce transfert de données PNR est mondial :
- « Pour le moyen et le plus long terme, les députés proposent une approche plus cohérente, au niveau de l'Organisation de l'aviation civile internationale (OACI), de

l'échange de données de passagers afin de garantir à la fois la sécurité du trafic aérien et le respect des droits de l'homme au niveau mondial ²⁵ ».

- 19 Les contraintes extérieures rattachent donc l'objectif de « cohérence juridique » à un contexte bien plus vaste que le strict paysage européen. Mais il rencontre aussi des difficultés à l'intérieur même de l'Union européenne.

Les difficultés

- 20 La « cohérence juridique » du programme européen en matière de technologies de sécurité se heurte à des difficultés d'ordre technique mais aussi à la réticence de certains Etats : le fait d'instituer entre les Etats des normes techniques identiques n'est pas encore acquis ²⁶, pas plus que la possibilité de connexion, nécessaire au fonctionnement commun des bases de données en matière de sécurité. Face à ces difficultés, la Commission a publié deux textes :

- 21 - l'un sur « le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergie entre ces bases » (communication de la Commission, 24 novembre 2005), position que le CEPD avait déjà critiqué sévèrement :

« La Commission considère que l'interopérabilité est un concept technique plutôt que juridique et politique. Cette confusion est déroutante et ne sert qu'à éviter les questions fondamentales. Les systèmes interopérables augmentent les risques pour les citoyens [...] il est essentiel d'examiner cela avec plus de prudence et de ne pas cacher la problématique derrière sa technicité ».

- 22 - l'autre est une proposition de décision-cadre tout-à-fait significative, visant l'échange d'information en vertu du principe de disponibilité ²⁷. Ce très diplomatique « principe de disponibilité » est en quelque sorte une réponse de repli, une proposition a minima face aux difficultés que rencontre l'UE dans son processus de « cohérence juridique » en matière de sécurité. Le principe de disponibilité est conçu comme étant un nouveau principe juridique important, la proposition de la Commission « ne s'inspir[ant] pas d'un modèle existant ; elle recommande au contraire une toute nouvelle approche » qui serait introduite par le programme de La Haye « selon lequel les informations nécessaires dans le cadre de la lutte contre la criminalité doivent pouvoir traverser sans entraves les frontières extérieures de l'UE ». Sont visées notamment, de manière nouvelle, les connexions entre des fichiers nationaux en matière génétique ²⁸. Le très diplomatique « principe de disponibilité » apparaît néanmoins être une création juridique destinée à pallier les obstacles de tous ordres existant face à son objectif de « cohérence juridique », et surtout face aux réticences de certains Etats membres.

- 23 En effet, antérieurement à ces textes, impatients face à la lenteur de la mise en place d'une coopération plus effective entre les Etats, ou au contraire désireux de contourner les difficultés et surtout les contraintes de la mise en œuvre de la « cohérence juridique » réclamée par l'Union européenne, sept Etats membres ont décidé de mettre en œuvre entre eux, dans le cadre d'un traité classique, des mesures leur permettant d'effectuer de tels échanges de données biométriques : le 27 mai 2005, un traité est signé par sept Etats de l'Union à Prüm, parfois désigné comme le « Schengen III », selon le processus qui avait déjà été suivi pour le premier accord de Schengen, donc en dehors de l'Union européenne ²⁹. L'objectif du traité est d'assurer une coopération transfrontalière efficace entre ces pays dans la lutte et la poursuite contre la criminalité grave. Dans ce but, le traité de Prüm vise à faciliter et à accélérer l'échange d'informations entre les autorités de poursuite des Etats parties au traité ³⁰, notamment

la recherche et comparaison automatisées des profils d'ADN dans la base de données des autres parties contractantes ³¹.

- 24 Ce contournement patent des obligations liées au programme européen de « cohérence juridique » rappelle que cet objectif de cohérence vise aussi à mettre en place des normes en matière de protection des droits fondamentaux, sans doute conçues a minima mais ayant le mérite d'exister et surtout de pouvoir être contrôlées par un juge, la Cour de justice des communautés européennes. Or, l'absence de fonctionnement démocratique dans le cadre de Schengen a souvent été dénoncée et l'on peut penser que, sans institution européenne encadrant le fonctionnement du traité de Prüm, on se heurtera aux mêmes insuffisances.
- 25 En conclusion, on se réfèrera aux nouveaux objectifs des projets de recherche consacrés à la biométrie financés par la Commission européenne dans le cadre du BITE. Selon J.-M. Manach :
- « la Commission européenne, après avoir financé 28 projets de recherche consacrés à la biométrie entre 1998 à 2003, s'était en effet aperçu que la majeure partie d'entre eux faisaient part de leur besoin d'un corpus éthique en la matière, qu'il s'agisse des implications de la centralisation de données biométriques, ou encore des risques de détournement de telles informations ».
- 26 C'est pourquoi elle a procédé à une consultation publique d'experts dans ce domaine jusqu'au 13 juin 2006, consultation dont elle attend les conclusions. Il semble que la précipitation des institutions européennes et des Etats à recourir à la biométrie se heurte désormais à des difficultés tant d'ordre technique (ainsi, le recours aux visas biométriques intégrés dans les passeports a été abandonné) que dans le domaine de la protection des droits fondamentaux, avec l'émergence d'une résistance nouvelle des individus, dont il ne faut toutefois pas surestimer les effets.

NOTES

1.. *Livre vert sur la convergence des secteurs des télécommunications, des médias et des technologies de l'information, et les implications pour la réglementation - Vers une approche pour la société de l'information*, COM(97) 623 final. Non publié au Journal officiel.

2.. Titre IV du traité de Rome tel que modifié par le traité d'Amsterdam : « Espace de liberté, de justice et de sécurité » où ont été transférées les politiques de visas, de contrôle aux frontières extérieures, d'asile et d'immigration (pour le moment toujours soumises à la règle de l'unanimité) – Titre VI du traité sur l'Union européenne : « Coopération policière et judiciaire pénale ». L'objectif de cet article n'étant pas de rappeler le fonctionnement complexe de ce système, on se reportera par exemple à l'étude : « Politique européenne d'asile et d'immigration », *Dictionnaire permanent droit des étrangers* (Conseillère scientifique : S. Preuss-Laussinotte). Pour une présentation synthétique de l'espace pénal européen, concerné aussi par les technologies de sécurité, voir Domenach J., « Quel avenir pour l'espace pénal européen : réflexions sur la nature des relations entre l'Union et les Etats membres dans le domaine pénal », *LPA*, 18 juillet 2006, n°142, p. 9.

- 3.. Règlement (CE) n°1683/95 du Conseil, du 29 mai 1995, établissant un modèle type de visa Journal officiel n° L 164 du 14/07/1995 p. 0001 – 0004.
- 4.. Pour une présentation de ces bases de données européennes, voir dans ce numéro : « Bases de données personnelles et politiques de sécurité : une protection illusoire ? ».
- 5.. Système d'information sur les visas : Décision 2004/512/CE du 19 février 2004 du Conseil portant sur la création du système d'information sur les visas (VIS).
- 6.. Communication de la Commission au Conseil et au Parlement européen COM/2003/0771 final : Le développement du système d'information Schengen II et les synergies possibles avec un futur système d'information sur les visas (VIS).
- 7.. Communication de la Commission au Conseil et au Parlement européen sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases, 24.11.2005 COM(2005) 597 final. Il est intéressant de noter qu'à l'origine, en 1997, malgré les réticences des Etats et des institutions de l'Union, c'est le Parlement européen qui voulait que n'existe qu'une seule base de données européenne, qu'il désignait sous le vocable « SIE » (système d'information européen).
- 8.. Selon le représentant de SAGEM – entreprise très impliquée dans ces programmes biométriques –, M. Bernard Didier, directeur scientifique et du développement des affaires (division Sécurité de Sagem Défense Sécurité, groupe SAFRAN) in « Compte rendu de l'audience publique du 4 mai 2006 sur la biométrie », Office parlementaire d'évaluation des choix scientifiques et technologiques. TWIC : Transportation Workers Identification Credential ; PIV : Vérification d'identification personnelle.
- 9.. Ibrügger L., Rapport de la Sous-Commission sur la prolifération des technologies militaires « Technologie et terrorisme », OTAN, Session annuelle, 2002.
- 10.. Le 11 juillet 2005, après les attentats de Londres, l'OACI publiait un communiqué de presse : « Les 188 Etats contractants de l'OACI sont convenus que tous les Etats doivent commencer à délivrer des MRP conformes à la norme de l'OACI au plus tard le 1er avril 2010 ».
- 11.. Dans le programme de La Haye, l'objectif prioritaire de l'Union européenne est d'intégrer à court terme les identificateurs biométriques dans les documents de voyage, les visas, les permis de séjour, les passeports des citoyens de l'Union européenne et les systèmes d'information, et à préparer la mise au point de normes minimales pour les cartes d'identité nationales « tenant compte des normes de l'Organisation de l'aviation civile internationale (OACI) ».
- 12.. « Article 22 Simplification des formalités. Chaque Etat contractant convient d'adopter, par la promulgation de règlements spéciaux ou de toute autre manière, toutes mesures en son pouvoir pour faciliter et accélérer la navigation par aéronef entre les territoires des Etats contractants et éviter de retarder sans nécessité les aéronefs, équipages, passagers et cargaisons, particulièrement dans l'application des lois relatives à l'immigration, à la santé, à la douane et au congé.
- Article 23 Formalités de douane et d'immigration. Chaque Etat contractant s'engage, dans la mesure où il le juge réalisable, à établir des règlements de douane et d'immigration intéressant la navigation aérienne internationale, conformément aux pratiques qui pourraient être établies ou recommandées en vertu de la présente Convention.
- Article 37 Adoption de normes et procédures internationales. Chaque Etat contractant s'engage à prêter son concours pour atteindre le plus haut degré réalisable d'uniformité dans les règlements, les normes, les procédures et l'organisation relatifs aux aéronefs, au personnel, aux

voies aériennes et aux services auxiliaires, dans toutes les matières pour lesquelles une telle uniformité facilite et améliore la navigation aérienne.

A cette fin, l'OACI adopte et amende, selon les nécessités, les normes, pratiques recommandées et procédures internationales traitant des sujets suivants : [...] b/ caractéristiques des aéroports et des aires d'atterrissage ; [...] j/ formalités de douane et d'immigration [...] et, lorsqu'il paraît approprié de le faire, de tout autre sujet intéressant la sécurité, la régularité et l'efficacité de la navigation aérienne ».

13.. Chaque type de MRTD contient, dans un format standard, des détails sur l'identité du détenteur, dont une photographie ou une image numérique. Les éléments d'identification obligatoires (la photographie de face et, désormais, l'empreinte digitale) sont reproduits dans une zone de lecture automatique (ZLA) de deux lignes imprimées dans le style « Reconnaissance optique de caractères-B (ROC-B) ». La normalisation des éléments présentés dans les documents de voyage permet aux pays participants dotés de lecteurs configurés selon le même standard ISO de lire la zone de lecture automatique des MRTD produits par tous les pays qui émettent le même type de document. A l'heure actuelle, les MRTD comprennent les passeports lisibles à la machine (MRP), les visas lisibles à la machine (MRV) et les documents de voyage officiels lisibles à la machine (TD).

14.. Règlement (CE) n°2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres.

15.. Règlement (CE) n°1030/2002 du Conseil du 13 juin 2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers JOUE n°L 157 du 15/06/2002.

16.. Michel Beland, expert en sécurité et sûreté de l'Organisation internationale de l'aviation civile, in « Compte rendu de l'audience publique du 4 mai 2006 sur la biométrie », Office parlementaire d'évaluation des choix scientifiques et technologiques.

17.. Avis du 16 octobre 2006 sur la Proposition de règlement du Conseil modifiant le règlement (CE) n°1030/2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers [COM(2003) 0558].

18.. Malgré les assurances des entreprises affirmant que « Cette clé ne peut être lue que par un lecteur légitime qui fera la lecture numérisée du passeport avec la puce, dans la zone de lecture automatique. Il faut donc que le passeport soit ouvert et qu'il soit sous le lecteur pour que la clé donne accès aux données biométriques numérisées. Le détenteur peut être assuré que les données sont protégées tant et aussi longtemps que le passeport est fermé et tant et aussi longtemps que le passeport n'est pas remis à l'officier de police pour contrôle », Michel Beland, *op. cit.*

19.. Voir dans ce numéro : « Bases de données personnelles et politiques de sécurité : une protection illusoire ? ».

20.. Décision 2004/535/CE de la Commission, du 14 mai 2004, relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des Etats-Unis d'Amérique (JO L 235, p. 11). L'article 25 de la directive du 24 octobre 1995 exige que tout transfert de données personnelles vers des Etats tiers à l'Union européenne ne peut s'effectuer que si ceux-ci possèdent une protection « adéquate » en matière de données personnelles, alors que les Etats de l'UE doivent disposer d'une

protection « équivalente » beaucoup plus exigeante, respectant la directive de 1995 ; l'appréciation de cette condition d'adéquation est confiée à la Commission européenne.

21.. Avis 8/2004 sur l'information pour les passagers concernant le transfert des données PNR sur les vols entre l'Union européenne et les Etats-Unis d'Amérique du 30 septembre 2004.

22.. CJCE 30 mai 2006, affaires jointes C-317/04 et C-318/04 Parlement européen / Conseil de l'Union européenne et Parlement européen / Commission des Communautés européennes.

23.. Décision 2006/729/PESC/JAI du Conseil du 16 octobre 2006 relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et les Etats-Unis d'Amérique sur le traitement et le transfert de données contenues dans les dossiers des passagers (données PNR) par des transporteurs aériens au ministère américain de la sécurité intérieure, JOUE L 298 du 27.10.2006.

24.. Recommandation du Parlement européen au Conseil concernant les négociations en vue de la conclusion d'un accord avec les Etats-Unis sur l'utilisation des données des dossiers passagers (PNR) dans le but de prévenir et de combattre le terrorisme et la criminalité transnationale, et notamment la criminalité organisée, INI/2006/2193, 7 septembre 06.

25.. Résolution non législative, PE, 7 septembre 06.

26.. En France par exemple, ces normes ne sont pas identiques pour l'ensemble des agences de sécurité, et l'interconnexion de leurs fichiers n'est pas autorisée pour le moment même si, à terme, celle-ci devrait être réalisée.

27.. Proposition de décision-cadre relative à l'échange d'informations en vertu du principe de disponibilité, 12 octobre 2005.

28.. Cet objectif n'est toutefois pas récent : dans une résolution adoptée en juin 1997, le Conseil des ministres de l'Union européenne avait encouragé la « création de bases de données ADN nationales », et « les échanges des résultats des analyses d'ADN [...]. Il appartient à chaque Etat membre de décider dans quelles conditions et pour quels délits les résultats des analyses ADN peuvent être stockés dans une base de données nationale [...] la création d'une base de données ADN européenne devra être considérée comme une deuxième étape, à réaliser une fois réunies les conditions (techniques) nécessaires à l'échange des analyses d'ADN ».

29.. Traité entre le royaume de Belgique, la République fédérale d'Allemagne, le royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le royaume des Pays-Bas et la République d'Autriche, relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, signé à Prüm le 27 mai 2005.

30.. Voir note 23.

31.. Pour d'intéressants articles sur le traité de Prüm, on se reportera à : Balzacq T., Bigo D., Carrera S., Guild E., *Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats*, Brussels, CEPS, 2006 ; Dehousse F., Sifflet D., *Les Nouvelles Perspectives de la coopération Schengen : le Traité de Prüm*, Royal Institute for International Relations (IRRI KIIB), 8 avril 2006. Voir aussi, plus récemment : Balzacq T., « From a Prüm of 7 to a Prüm of 8: What are the Implications? », *Directorate-General Internal Policies, Policy Department C, Citizens Rights and Constitutional Affairs*, 4 décembre 2006.

RÉSUMÉS

Cet article vise à analyser, sous l'angle juridique, le rôle de l'Union européenne dans le choix des technologies de sécurité, choix qui s'est essentiellement traduit par le recours à la biométrie et aux bases de données, deux éléments indissociables. Ce choix l'a été dans un objectif de « cohérence juridique » présenté comme nécessaire pour l'élaboration d'une politique européenne de sécurité. Mais la réalisation de cet objectif reste contrainte par une série de décisions extérieures à l'Union, notamment celles des Etats-Unis et de l'OACI. Il se heurte de plus à la réticence de certains Etats, et à la difficulté de mise en œuvre de cette « cohérence juridique », même en créant un « principe de disponibilité » complexe entre les Etats.

This article seeks to analyze, from a legal angle, the role played by the European Union in the adoption of technologies of security involving the resort to two inseparable elements: biometrics and databases. This choice has been part of the objective of "legal coherence" and is presented as necessary for the development of a European security policy. But the realization of this aim is constrained by decisions taken outside of the EU, precisely in the US and at the ICAO. It is also constrained by the reluctance of certain member states as well as by the difficulties raised by the implementation of this "juridical coherence" and this in spite of the complicated "principle of availability" that has been established between the Member States.

INDEX

Index géographique : Europe

Mots-clés : bases de données, biométrie, construction européenne

AUTEUR

SYLVIA PREUSS-LAUSSINOTTE

Sylvia Preuss-Laussinotte est maître de conférences en droit public à Paris-X Nanterre, directrice du Master 2 « Droit des nouvelles technologies et société de l'information » et titulaire d'un DEA de sociologie de l'EHESS.