Pièce d'identité des gens de mer

Patrick Chaumette

Neptunus, revue électronique,
Centre de Droit Maritime et Océanique, Université de Nantes,
Vol. 14, 2008/1
http://www.cdmo.univ-nantes.fr/centre-droit-maritime-oceanique/cdmo

2è Colloque International
Sûreté maritime
Code ISPS International Ship and Port facility Security

Entre devoirs citoyens et obligations économiques
Between citizen duty and business pressure
Entre obligaciones ciudadanas y compromisos económicos
Colloque organisé par le port autonome de Nantes Saint-Nazaire
et l'Ecole de la Marine Marchande de Nantes

27-28 septembre 2007
Cité des Congrès, Nantes

Pièce d'identité des gens de mer.

Patrick CHAUMETTE
Professeur de droit à l'Université de Nantes

De la sûreté.
Le passé récent (paquebot *Aquille Lauro* en 1985, pétrolier *Limbourg* en 2002) a démontré qu'aucun pays au monde n'est à l'abri d'actions terroristes, d'actes illicites, et le transport maritime n'échappe pas à la règle. Il est nécessaire de garantir à tout moment la sûreté du transport maritime, celle des citoyens qui l'utilisent et celle de l'environnement, face à des menaces d'actions illicites internationales comme le terrorisme. Lors du transport de marchandises contenant des substances dangereuses, les dangers suscités par ces actions illicites peuvent être lourds de conséquences pour les citoyens et pour l'environnement de l'Union Européenne[1].

A la suite des attentats de New York du 11 septembre 2001, l'Organisation Maritime Internationale a adopté, le 12 décembre 2002, le code international *for security of ships and ports* (ISPS) relatif à la sûreté des navires et des installations portuaires, qui révise la Convention SOLAS, *safety for life at sea*, et lui ajoute un nouveau chapitre 11; ce Code facultatif est entré en vigueur en France et devenu obligatoire, le 1er juillet 2004[2] ; le Règlement 725/2004 du Parlement européen et du Conseil du 31 mars 2004 l'impose aux

[1] P. Marionnet, *Sûreté maritime et portuaire. Vade-mecum ISPS*, InfoMer, Rennes, 2006 ; P. Polere, « Sûreté maritime : bilan et perspectives du code ISPS », *DMF* 2006, pp. 275-284 ; F-M. Torresi, « La repressione degli atti illeciti contro la sicurezza della navigazione marittima : attualità e prospettive si sviluppo", *Il Diritto Marittimo*, 2006, fasc. 3, pp. 758-777.

[2] D. n° 2004-290, 26 mars 2004, portant publication des amendements à l'annexe à la Convention internationale de 1974 pour la sauvegarde de la vie humaine en mer, *JO* 27-3-2004de 1974 pour la sauvegarde de la vie humaine en mer, *JORF* 27-3-2004

Etats membres de l'Union européenne[3]. Les zones d'interfaces navire/port doivent faire l'objet d'un plan de sûreté prédéfini, variant selon les divers niveaux d'alerte[4].

Le Règlement 725/2004 du 31 mars 2004 vise à fournir une base pour l'interprétation et la mise en œuvre harmonisées, ainsi que pour le contrôle communautaire des mesures spéciales pour renforcer la sûreté maritime adoptées par la conférence diplomatique de l'Organisation Maritime Internationale en 2002, modifiant la convention internationale de 1974 relative à la sauvegarde de la vie en mer (SOLAS) et instauration du code international relatif à la sûreté des navires et des installations portuaires (International Ship and Port Facility Security Code - code ISPS)[5]. Le Code ISPS est entré en vigueur le 1er juillet 2004[6].
En novembre 1993, l'OMI avait adopté le code international de la gestion de la sécurité des navires et la prévention de la pollution (code ISM : International Safety Management), qui a pour objet de mettre en place, au sein des compagnies maritimes, un système de gestion pour la sécurité de l'exploitation des navires et la prévention de la pollution. Ce code intégré au chapitre IX de la convention internationale sur la sauvegarde de la vie humaine en mer (SOLAS). L'application du code ISM est obligatoire pour tous les États membres[7]. Il s'impose à tous les navires de plus de 500 tonneaux, depuis le 1er juillet 2002. En 2003, la Commission a proposé une proposition de Règlement du Parlement européen et du Conseil relatif à l'application du code international de gestion de la sécurité dans la Communauté.

Des documents d'identité des gens de mer
La convention 185 de l'OIT, adoptée à Genève, le 19 juin 2003 est consécutive aux attentats aériens de New York de décembre 2001; elle porte sur les pièces d'identité des gens de mer. Elle a été ratifiée par la France par la loi n° 2004-146 du 16 février 2004[8]. Cette convention est entrée en vigueur le 9 février 2005 à la suite de la ratification de la France, de la Jordanie et du Nigeria[9]. L'article 2 de la convention demande à chaque Etat de fournir à ses

---

[3] Règlement n° 725/2004 du Parlement européen et du Conseil, 31 mars 2004, *JOUE L* 129, 29 avril 2004 ; Directive 2005/65/CE du Parlement européen et du Conseil, 26 octobre 2005 relative à l'amélioration de la sûreté des ports.
[4] P. Marionnet, *Sûreté maritime et portuaire. Vade-mecum ISPS*, InfoMer, Rennes, 2006.
[5] Règlement n° 725/2004 du Parlement européen et du Conseil, 31 mars 2004, relatif à l'amélioration de la sûreté des navires et des installations portuaires, *JOCE L* 129, 29 avril 2004, pp. 6-91 ; Directive 2005/65/CE du Parlement européen et du Conseil, 26 octobre 2005 relative à l'amélioration de la sûreté des ports.
[6] Décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale ; Décret n° 2007-476 du 29 mars 2007 du 29 mars 2007 relatif à la sûreté du transport maritime et des opérations portuaires, *JORF* n° 76, 30 mars 2007, p. 5949.
[7] A.M. Chauvel, *Sécurité en mer. Le code ISM*, Éd. Préventique, Bordeaux, 1996 : R. Cuisigniez, *La réglementation de sécurité à bord des navires*, InfoMer, Rennes, 2004 ; R. Baumler, « L'instrumentation des codes ISM et ISPS », *Annuaire de Droit Maritime et Océanique*, Université de Nantes, 2005, t. XXIII, pp. 95-108.
[8] L. n° 2004-146, 16 février 2004, autorisant la ratification des Conventions 163, 164, 166, 178, 179, 180, 185 de l'OIT et du protocole de 1996 relatif à la Convention 147, *JORF* 17-2-2004 p. 3167.
[9] *Travail*, magazine de l'OIT, n° 53, avril 2005, p. 35. Gw. Proutière-Maulion, « Les transports », *Droit des relations extérieures de l'Union européenne*, A. Fenet (dir.), Litec, coll. Objectif Droit, 2006, n° 450 et s., p. 205 et s ; ratification des Bahamas, 14 décembre 2006, du Pakistan, 21 décembre 2006, de la République de Corée, 4 avril 2007, de

ressortissants, exerçant la profession de marin, qui en font la demande, une pièce d'identité conforme, comportant des données biométriques ; un enregistrement de chaque pièce d'identité délivrée, suspendue ou retirée par lui, doit être conservé dans une base de données électronique. Un centre permanent doit être accessible en vue de vérifications. Cette carte doit être lisible par un lecteur SID (Seafarers' Identity Documents), tel qu'ils s'en trouvent dans les aéroports.

Les titulaires de ces documents devraient obtenir plus facilement l'autorisation de descendre à terre pendant une escale ou aux fins de transit et de transfert, en dépit des mesures de sûreté maritime et portuaire, liés au *Code International Ship and Port facilicity Security,* ISPS, de l'Organisation maritime internationale[10].

Le Titre IV du Traité de l'Union européenne porte sur les visas, l'asile, l'immigration et les autres mesures relatives à la libre circulation des personnes dans la Communauté (art. 62 et 63). Spécialement, l'article 62, § 2-b-i prévoit l'adoption d'une liste de pays tiers dont les ressortissants sont soumis à l'exigence de visas pour franchir une frontière extérieure de la Communauté. La Communauté européenne a exercé ses compétences en adoptant le Règlement (CE) du Conseil nº 539/2001 du 15 Mars 2001. Les articles 6.5.2 et 6.5.4 de la seconde partie du Manuel commun des frontières extérieures font référence aux conditions dans lesquelles les marins peuvent entrer sur le territoire des Etats membres pour de courts séjours liés aux transits, transferts et rapatriements.

Le Conseil de l'Union européenne a décidé le 14 avril 2005 d'autoriser les Etats membres à ratifier dans l'intérêt de la Communauté européenne cette convention internationale, dans le cadre de la politique commune en matière de visas[11]. La Communauté ne peut ratifier la convention de l'OIT ; elle ne peut adhérer à cette institution en raison du caractère tripartite de celle-ci ; seuls les Etats membres peuvent ratifier une convention de l'OIT. La France n'aurait pas dû ratifier cette convention internationale sans l'autorisation du Conseil de l'Union européenne. Il existe actuellement 12 ratifications, dont celle de la Hongrie et de la Lituanie. Cette autorisation a permis la transmission de la ratification française au conseil d'administration du Bureau International du Travail.

En 2004, le conseil d'administration du BIT a approuvé une norme de conversion de deux empreintes digitales en un gabarit biométrique, numérisé dans un code-barres bidimensionnel, qui doit être normalisé à l'échelle internationale et imprimé sur la pièce d'identité des marins. Le système doit être caractérisé par une interopérabilité sur le plan mondial, les informations étant lisibles dans tous les ports du monde, à l'avenir. Deux produits ont été retenus en décembre 2004 par le BIT, à la suite de six semaines d'essais, d'où une norme du BIT, SID-0002. Plus de 50 pays ont mis en œuvre une procédure de ratification.

Madagascar, 6 juin 2007, de l'Albanie, 11 octobre 2007, du Nigéria et de l'Indonésie, décembre 2007. La ratification de la Fédération de Russie est en chemin.

[10] Code International pour la sûreté des navires et des installations portuaires, 12 décembre 2002, OMI, London.

[11] Décision 2005/367 du Conseil, *JOUE* n° L 136, 30-5-2005 p. 1 ; le Royaume-Uni et l'Irlande ne font pas partie de cette politique commune des visas ; le Danemark, en dépit des réserves émises quant aux règlements communautaires de droit international privé, est destinataire de cette décision.

L'article 2 de la convention 185 demande à chaque État de fournir à ses ressortissants, exerçant la profession de marin, qui en font la demande, une pièce d'identité conforme, comportant des données biométriques, visibles sur la pièce d'identité ; un enregistrement de chaque pièce d'identité délivrée, suspendue ou retirée par lui, doit être conservé dans une base de données électronique (art. 4). Les gens de mer doivent disposer d'un accès facile à des équipements leur permettant d'examiner toute donnée les concernant, qui peut faire l'objet d'un examen visuel (art. 4 et 5). Cette pièce d'identité est un document autonome et n'est pas un passeport. Les titulaires de ces documents devraient obtenir plus facilement l'autorisation de descendre à terre pendant une escale ou aux fins de transit et de transfert, en dépit des mesures de sûreté maritime et portuaire, liés au Code International Ship and Port facility Security, ISPS, de l'Organisation maritime internationale (art. 6). Les gens de mer ne sont pas tenus d'être en possession d'un visa pour être autorisés à descendre à terre. La pièce d'identité reste en possession en permanence du marin, sauf lorsqu'elle est sous la garde du capitaine, avec l'accord écrit du marin (art. 7). Le problème est moins la fabrication de ces documents d'identité comportant des données biométriques, que le contrôle de leur utilisation, sans falsification, ce qui nécessite la diffusion de lecteurs appropriés dans les divers ports du monde. La lecture dans les aéroports semble aisée, compte tenu des évolutions intervenues dans la sûreté aérienne notamment à partir de l'accident de Lockerbie, attentat attribué aux services libyens

Livret maritime et document d'identité.

L'autorité maritime délivre gratuitement au marin un livret professionnel qui mentionne l'engagement, sans contenir aucune appréciation des services rendus, ni aucune indication sur les salaires (C. trav. mar., art. 14 - Conv. OIT, n° 22 de 1926, art. 8)[12]. Ce livret mentionne les brevets et diplômes, les visites médicales d'aptitude à la navigation, la stabilisation du marin dans son entreprise. Ce livret constituait une preuve de l'appartenance à l'équipage, il était devenu une pièce d'identité, un véritable passeport, un document international de circulation (Conv. OIT, n° 108 de 1958)[13].

Il est apparu nécessaire de distinguer avec soin la pièce d'identité du marin et son livret professionnel maritime, qui constate ses engagements professionnels.

L'arrêté ministériel du 24 janvier 2007 rappelle que le livret professionnel maritime est délivré et renouvelé gratuitement par l'administration au marin ; en cas de perte ou de vol, il ne sera délivré un nouveau livret que sur demande, accompagnée d'un justificatif de déclaration de perte ou de vol. Le livret ne peut contenir aucune appréciation de la qualité du travail du marin, des services rendus, ni aucune indication sur ses salaires ; le marin peut faire mentionner la date du début de son contrat d'engagement[14].

Des documents d'identité à données biométriques.

De la protection des données personnelles et de la protection de la vie privée.

[12] Convention OIT, n° 22 de 1926.

[13] Convention OIT, n° 108 de 1958.

[14] Arrêté 24 janvier 2007, *JORF* 10 février 2007, p. 2566.

En Espagne, la ratification de la Convention 185 semble soulever des difficultés constitutionnelles, en raison de l'ampleur du principe de protection de la vie privée, de « la intimidad »[15].
En France, il s'agit d'une question de méthode, plus qu'une question de principe[16]. Depuis 1984, date de création du Fichier National des Empreintes Digitales, premier dispositif biométrique à lui avoir été présenté, la CNIL, Commission nationale de l'informatique et des libertés, examine chaque dispositif en prenant en compte les caractéristiques de la biométrie utilisée et les risques qu'elle comporte pour les libertés individuelles et la protection des données personnelles. A cet égard, la CNIL n'autorise l'enregistrement des empreintes digitales dans une base centralisée que si cette technologie se justifie par un "fort impératif de sécurité". Il s'agit, par exemple, du contrôle de l'accès aux sites nucléaires.

La consultation de la CNIL, Commission nationale de l'informatique et des libertés, s'impose au Ministère de l'Equipement et des Transports. Il s'agit pour la France de produire des documents à destination des marins, ressortissants nationaux, et de gérer une base nationale de données. L'évolution vers des passeports contenant des données biométriques a ouvert la voie. Il s'agit ensuite de lire dans les aéroports notamment les pièces d'identité des gens de mer étrangers, en transit. Si les opérateurs portuaires entendent s'équiper de lecteurs afin de veiller au contrôle des déplacements, ces contrôles glissent de la sphère publique vers la sphère privée. Les pratiques mises en œuvre dans les zones de sûreté aéroportuaires ou les zones d'accès restreint, donnent ici des lignes directrices connues, qu'il conviendra de compléter.

Biométrie. La Commission nationale de l'informatique et des libertés (CNIL) est défavorable à la création de bases de données d'empreintes digitales sur les lieux de travail ; elle encadre strictement les autres utilisations de données biométriques.
Le 8 avril 2004, elle a confirmé sa position antérieure. A la différence d'autres données biométriques, les empreintes digitales laissent des traces pouvant être exploitées pour l'identification des personnes, mais susceptibles d'être utilisées à des fins étrangères à cet objectif d'identification. Si le gabarit de l'empreinte digitale est uniquement stocké dans un support personnel, le dispositif ne pose pas de difficultés, en l'absence de risque important de détournement. Il en va de même des dispositifs recourant aux biométries ne laissant pas de traces, telles la reconnaissance du contour de la main ou de l'iris de l'œil. Ainsi, le dispositif du contrôle d'accès aux zones réservées de sûreté d'Orly et de Roissy a été autorisé, en raison de l'absence de stockage des données biométriques sur un lecteur central, du respect du principe de proportionnalité quant à l'enregistrement et la conservation des données de passage, de la limitation des destinataires de ces informations, de l'information individuelle et collective assurée aux salariés concernés (*Délib. CNIL n° 04-017, 8 avril 2004*, http://www.cnil.fr). Cette appréciation a été confirmée *(Délib. CNIL n° 2006-102, 27 avril 2006 : JORF, 16 juin)*. Un avis défavorable a en revanche été donné au système envisagé par un centre hospitalier, lié au contrôle des temps de travail du personnel, sans stockage de l'empreinte digitale sur le support individuel, de sorte que les personnels n'avaient aucune

[15] O. Fotinopoulou-Basurko, « El documento de identidad de la gente de mar : Seguridad en las fronteras y derecho a la intimidad », Annuaire de Droit maritime et Océanique, Université de Nantes, pp. 157-171.
[16] Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi n° 2003-239 du 18 mars 2003 (JORF 19 mars 2003) et révisée par la Loi n° 2006-64 du 23 janvier 2006 (*JORF* 24 janvier 2006).

maîtrise sur le lecteur biométrique central (*Délib. CNIL n° 04-018, 8 avril 2004*, http://www.cnil.fr).
L'utilisation de techniques biométriques recourant aux empreintes digitales pour contrôler l'activité des salariés ne saurait être admise que dans des hypothèses très particulières ; utilisé pour contrôler le temps effectif de travail des salariés exerçant leur activité dans un espace public, ce dispositif n'est ni adapté, ni proportionné au but recherché et doit être interdit *(TGI Paris, 1re ch., 19 avril 2005, n° 05/00382, Comité d'entreprise d'Effia Services et Fédération des syndicats SUD Rail c/ Sté Effia Services)*.
La reconnaissance du contour de la main est une technique biométrique qui ne laisse pas de traces et donc ne soulève pas de difficultés au regard de la loi informatique et libertés. Les lecteurs biométriques contiennent une base de données comportant les gabarits biométriques et les codes d'accès. Lors de chaque passage, la reconnaissance du contour de la main s'opère après saisie sur le clavier du lecteur d'un code personnel, en plaçant la main sur un appareil de capture de l'image géométrique de la main. Aucune image ou photo de la main n'est conservée. Seule une clé biométrique (chaîne de caractères), résultat du traitement de mesures par un algorithme, est associée à l'identité de la personne. A la différence des empreintes digitales, le contour de la main ne laisse pas de traces susceptibles d'être utilisées à des fins étrangères à la finalité recherchée par le responsable du traitement. Ce dispositif paraît donc actuellement adapté et proportionné à la finalité assignée *(CNIL 29 juill. 2005, Biométrie & contour de la main : http://www.cnil.fr)*. La CNIL a simplifié les formalités des dispositifs biométriques ayant recours au contour de la main pour le contrôle d'accès, la gestion des horaires et la restauration sur les lieux de travail *(Délib. CNIL n° 2006-101, 27 avr. 2006 : JORF, 16 juin)*.

De l'enregistrement des documents d'identité et de la constitution de fichiers ?
Quelle traçabilité des déplacements terrestres des gens de mer ? Il peut être tentant de constituer des fichiers de marins.

Les passagers aériens ont fait l'objet d'accords internationaux de transmission des données personnelles[17]. Ces accords internationaux créent des souplesses à la protection communautaire et nationale des données personnelles[18]. Selon le site de la Commission nationale Informatique et Libertés, du 3 août 2007, « Le nouvel accord Europe/Etats-Unis sur les données des passagers aériens est au détriment des citoyens européens » (http://www.cnil.fr/index.php?id=2241). « Les négociations entre les Etats-Unis et l'Union européenne ont mis un terme à plusieurs années d'incertitude quant aux conditions dans lesquelles les autorités des Etats-Unis accèdent aux données des passagers aériens européens

[17] Décision du Conseil n° 2007/551/PESC/JAI, 23 juillet 2007, relative à la signature au nom de l'Union européenne d'un accord entre l'UE et les USA sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au Ministère US de la sécurité intérieure (DHS), *JOUE* n° L 204, 4 août 2007, p. 16 et s.
[18] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *JOCE* L 281, 23 novembre 1995, pp. 31–50 ; Directive européenne 2002/58/CE du 12 juillet 2002 du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *JOUE L 201, 31 juillet 2002, pp. 37–47*.

(« données PNR »). L'accord, qui vient d'être conclu entre les Etats-Unis et l'UE, revient sur de nombreuses garanties défendues par les CNIL européennes.
Les données PNR («Passenger Name Record») sont des informations collectées auprès des passagers aériens au stade de la réservation commerciale. Elles permettent d'identifier l'itinéraire du déplacement, les vols concernés, le contact à terre du passager (numéro de téléphone au domicile, professionnel, etc.), les tarifs accordés, le numéro de carte bancaire du passager, ainsi que les services demandés à bord tels que des exigences alimentaires spécifiques (végétarien, asiatique, cascher, etc.) ou des services liés à l'état de santé du passager.

Peu après les attentats du 11 septembre, les Etats-Unis ont mis en œuvre de nouvelles dispositions en matière de sécurité de l'aviation et du transport, et des conditions d'entrée sur le territoire américain. Dans ce cadre, les compagnies aériennes ont l'obligation de communiquer aux services des douanes et de sécurité américains les données PNR de leurs passagers à destination des Etats-Unis. Le non respect de ces obligations est sanctionné par des contrôles renforcés, d'amendes et du refus du droit d'atterrir. L'accès aux données PNR détenues par les compagnies aériennes européennes est actuellement régi par un accord international transitoire, venant à expiration le 31 juillet prochain.

Le nouvel accord, qui devait entrer en vigueur au 1er Août 2007, est composé de l'accord proprement dit, et d'une lettre du ministère américain de l'intérieur (DHS) qui précisera certains points de l'accord. Une fois ratifié par les Parlements nationaux, cet accord transatlantique entrera en vigueur pour une durée de 7 ans. Les négociations sur cet accord ont été marquées par des exigences américaines toujours croissantes. Les craintes exprimées à de nombreuses reprises par la CNIL et ses homologues européens, réunis au sein du groupe dit « de l'article 29 », auprès des gouvernements des pays de l'UE et de la Commission européenne se sont malheureusement confirmées.
Le nouvel accord devrait en effet consacrer les dispositions suivantes :

* Le nombre d'autorités américaines qui pourront accéder aux données PNR sur le territoire américain a été étendu ;
* Les finalités d'utilisation des données PNR pourront varier en cas de modification unilatérale de leur législation par les Etats-Unis ;
* La décision éventuelle de transférer des données PNR européennes vers d'autres pays tiers sera prise de manière unilatérale par les Etats-Unis, sans consultation préalable des autorités européennes ;
* Il est désormais possible aux autorités des Etats-Unis, « en cas de nécessité », d'avoir accès à des données dites « sensibles », c'est-à-dire pouvant révéler l'origine raciale, ethnique, les opinions politiques, l'état de santé des personnes, malgré un filtrage initialement prévu ;
* Les données seront conservées non plus 3 ans 1⁄2 mais 15 ans, sous forme d'une conservation « active » pendant 7 ans et « passive » pendant 8 ans, sans garantie que les fichiers non consultés soient définitivement détruits ;
* Le passage du mode « pull » actuellement en vigueur (c'est à dire l'accès direct par les autorités américaines aux données détenues par les compagnies aériennes) au mode « push » (c'est à dire l'envoi des données par les compagnies aériennes, ne permettant plus d'accès direct aux autorités américaines) ne sera réalisé au 1er janvier 2008 que si les conditions techniques de ce passage paraissent acceptables aux Etats-Unis ;
* L'évaluation de l'application de l'accord (« review ») perd son caractère annuel obligatoire. Seul le commissaire européen de la Direction Générale Justice-Liberté-Sécurité sera en charge de cette inspection, sans que les autorités nationales de protection des données

y soient clairement associées ;

* Les autorités américaines auront la faculté de décider de manière unilatérale s'il sera répondu favorablement aux demandes des passagers européens d'accès et de rectification aux données les concernant détenues par les autorités américaines.

Le nouvel accord met un terme à la période d'incertitude ouverte par la décision de la Cour de Justice des Communautés Européennes du 30 mai 2006 annulant le précédent accord conclu le 28 mai 2004. Cependant, d'après les autorités européennes de protection des données, le Parlement européen et le Contrôleur européen, cet accord est loin d'offrir un niveau de protection adéquat aux données PNR transmises. On ne peut que regretter l'insuffisance de dispositions claires et proportionnées relatives au partage d'informations, de conservation, d'envois supplémentaires de données, de contrôle par les autorités de protection des données, et s'inquiéter de ce que la mise en œuvre de nombreuses dispositions soit soumise à la discrétion des Etats-Unis. »

La Commission européenne souhaite modifier la décision-cadre de 2002 sur la lutte contre le terrorisme[19] et se doter, notamment d'un système de stockage des données personnelles des passagers aériens. A l'instar de l'administration des USA, les Etats membres pourraient bénéficier ainsi d'un système d'échanges de dossiers passagers (*Passenger Name Records* ou PNR) dans lesquels figureraient dix-neuf informations, dont les noms et adresses des voyageurs, leur adresse électronique, les numéros de téléphone, moyens de paiement, itinéraire complet du voyage, contacts à terre, les données médicales et le comportement alimentaire[20].

Le Traité de Prüm du 27 mai 2005 a été signé entre la Belgique, l'Allemagne, l'Espagne, la France, le Luxembourg, les Pays-Bas et l'Autriche ; il renforce la coopération transfrontalière en vue de lutter contre le terrorisme, la criminalité et l'immigration illégale. Il prévoit l'échange de données génétiques, d'empreintes digitales et de données à caractère personnel , dont les immatriculations de véhicules automobiles, entre les administrations des Etats concernés. Le Traité se réfère au cadre de protection des données personnelles établi par le Conseil de l'Europe. Ce Traité doit permettre à tous les Etats membres de l'Union européenne de participer, dans l'avenir, à cette coopération policière et entraide judiciaire. Cette convention internationale a été conclue en dehors de l'Union européenne, afin d'échapper aux lenteurs des processus décisionnels[21]. Toutefois, ce Traité s'inscrit dans le programme de La Haye de novembre 2004 de l'Union européenne visant à renforcer la liberté, la sécurité et la justice. Le conseil « justice et affaires intérieures » du 15 février 2007 a donné lieu à un fort consensus des 27 ministres de l'intérieur, à l'exception de la question des interventions de police transfrontalières.

Ce n'est qu'en apparence que ces questions semblent éloignées des documents d'identité des gens de mer et de leurs facilités de circulation.

---

[19] Décision-cadre n° 2002/475/JAI du Conseil, 13 juin 2002, *JOCE* n° L 164, 22 juin 2002.

[20] Communiqué de presse de la Commission n° IP/07/449, 6 novembre 2007.

[21] F. DEHOUSSE et D. SIFFLET, « Les nouvelles perspectives de la coopération de Schengen : le traité de Prüm », Studia Diplomatica, vol. 49, n° 2/2006, pp. 199-212 ; N. QUILLET, « Le Traité de Prüm relatif à l'approfondissement de la coopération transfrontalière », Rev. du Marché commun et de l'Union européenne 2007, n° 513, pp. 660-664.

Les USA entendent mettre en œuvre des mesures unilatérales concernant l'accès des marins dans leurs ports ou aéroports. Ainsi que l'a expliqué au colloque le représentant des US Coast Guards, le commandant J. MAIORINE, les marins susceptibles de toucher le territoire US devront disposer d'une carte d'autorisation, constituée à l'avance et dotée de données biométriques. Les gens de mer devant entrer sur le territoire US ou dans les eaux territoriales ne sont pas dispensés de visas depuis le 11 septembre 2001. Les listes d'équipage ne permettent plus la délivrance collective des visas. Les USA poursuivent leur stratégie d'origine : n'ayant pas pu obtenir de l'OIT une base mondiale des gens de mer, ils instituent une base mondiale des marins susceptibles de toucher le sol US, ce qui ouvre la porte à deux catégories de marins. Il existe des problèmes juridiques à la ratification par les USA de la Convention 185 de l'OIT. Ces difficultés portent sur l'exigence de visas et sur l'absence de confiance dans les documents d'identité produits par de nombreux Etats. Les marins devront être titulaire des cartes d'accréditation permettant l'accès aux zones sensibles. La loi MTSA (Maritime Transportation Security Act) d'application du Code ISPS impose la délivrance de cartes TWIC, *Transportation Worker Identification Credentials*[22]. 10.000 personnes sont actuellement concernées par ces établissements à hauts risques, mais au total ce sont entre 750.000 et 1,5 millions de personnes qui seront concernées. Cette extension est mise en œuvre depuis le 29 septembre 2007. Les normes US sont distinctes de celles de l'OACI (Organisation de l'aviation civile internationale). La carte TWIC est facturée 150 USD à son usager et valable 5 ans. En cas de perte, elle est renouvelée, mais facturée 60 USD à l'usager. La délivrance de cette carte TWIC donne lieu à des enquêtes éventuellement judiciaire, militaire et de renseignements. Le marin, souhaitant se rendre aux USA, devra être préalablement titulaire d'une carte TWIC.

Quels échanges seront issus de cette base de données des cartes TWIC ?

[22] *Currents*, Fall 2007, vol. 17, n° 1, The Seamen's Church Institute, New-York , USA, www.seamenschurch.org ; D. BLANCHARD, « Seafarers' Credentials and Terminal Access », 18 octobre 2006 ; D.B. STEVENSON, « TWICs Identify American mariners – what about the foreign mariners ? », 23 janvier 2007, www.seamenschurch.org/418.asp