Cultures & Conflits

60 | hiver 2005
L'action humanitaire : normes et pratiques

Contrôle des étrangers, des passagers, des citoyens : surveillance et anti-terrorisme

Valsamis Mitsilegas

Édition électronique
URL : http://journals.openedition.org/conflits/1829
DOI : 10.4000/conflits.1829
ISSN : 1777-5345

Éditeur :
CCLS - Centre d'études sur les conflits lilberté et sécurité, L'Harmattan

Édition imprimée
Date de publication : 1 décembre 2005
Pagination : 185-197
ISBN : 2-296-00230-7
ISSN : 1157-996X

Référence électronique
Valsamis Mitsilegas, « Contrôle des étrangers, des passagers, des citoyens : surveillance et anti-terrorisme », *Cultures & Conflits* [En ligne], 60 | hiver 2005, mis en ligne le 10 octobre 2005, consulté le 19 avril 2019. URL : http://journals.openedition.org/conflits/1829 ; DOI : 10.4000/conflits.1829

Contrôle des étrangers, des passagers, des citoyens : surveillance et anti-terrorisme

Valsamis Mitsilegas

1 Ces dernières années les demandes d'intensification de la surveillance et des contrôles du mouvement des personnes au niveau mondial se sont développées 1. Ces appels, menés en priorité par les Etats-Unis après les évènements du 11 septembre, ont été suivis par les Etats membres de l'Union européenne. Les attentats du 11 mars 2004 à Madrid ont redoublé de tels appels, et l'accent a de nouveau été mis sur la nécessité d'une action concertée par l'UE dans ce domaine. Catégorisés sous le titre de « sécurité frontalière », ces projets ont envisagé la transmission de données personnelles des passagers des pays tiers voyageant vers l'UE, et de l'UE aux EU, par les compagnies aériennes aux autorités responsables du contrôle des frontières et de la gestion de l'immigration. Ces projets ont pour objectif le dépassement de la sécurité frontalière, en incorporant des identificateurs biométriques aux visas et aux documents identitaires, et l'accroissement de la capacité technique et de la communication entre bases de données contenant ces informations de manière à en faciliter l'échange (dans l'UE le terme – pas très élégant – utilisé pour nommer ce phénomène est « l'interopérabilité »).

2 Cette intensification de la surveillance du mouvement, réalisée par l'élargissement (en augmentant les échanges des données personnelles) et l'approfondissement (en introduisant la biométrie) des contrôles, semble contredire certaines dynamiques à l'œuvre au sein de l'UE notamment en ce qu'elle se veut un espace de libre circulation et de faible contrôle aux frontières. Les mesures menant à cette intensification de la surveillance, mais aussi la manière par laquelle ces mesures ont été adoptées, posent des questions fondamentales sur la légitimité, la démocratie et la protection des droits de l'Homme au sein de l'UE. Ces questions se complexifient lorsqu'on intègre la dimension « globale » du recueil et de l'échange d'informations après le 11 septembre 2001. Cet

article abordera ces questions en analysant les négociations, le contenu et les conséquences des récents projets de l'UE en ce domaine.

3 Le projet de loi relatif à cette directive n'a pas été présenté par la Commission européenne mais par le gouvernement espagnol en mars 2003[2]. La première version prévoyait la transmission extensive, par les transporteurs aériens et maritimes, des données sur les passagers aux autorités responsables du contrôle des frontières à leur demande et avant le départ. Ces données incluaient *inter alia* le numéro et le type de document de voyage utilisé, la nationalité, le nom et la date de naissance du passager ainsi que le point de passage frontalier utilisé pour entrer sur le territoire des Etats membres. Le projet laissait aux Etats membres la discrétion de demander aux transporteurs de transmettre aux autorités responsables de la gestion de l'immigration les données relatives aux passagers qui n'avaient pas utilisé leur billet de retour. Les transporteurs désobéissants seraient « punis » par des sanctions monétaires[3].

4 Imposer des obligations additionnelles aux transporteurs n'était pas une priorité pour la Commission européenne dans le développement de l'action pour combattre l'immigration clandestine. En juin 2003, trois mois après la présentation du projet de loi API par le gouvernement espagnol, la Commission publia une communication[4] aux chefs des Etats européens qui s'apprêtaient à discuter à Thessalonique, dans le courant du mois, du développement d'une politique européenne commune en matière d'immigration clandestine. La Commission notait que de nouvelles mesures d'harmonisation sur la responsabilité des transporteurs n'étaient pas nécessaires pour le moment[5]. De même, les conclusions du Conseil européen de Thessalonique ne contenaient aucune référence à la responsabilité des transporteurs, ou à la nécessité d'intensifier la surveillance des passagers.

5 Cependant, malgré l'absence d'un accord généralisé dans l'UE sur de telles initiatives, certains Etats membres sont en faveur d'une intensification du contrôle des mouvements des personnes vers – et au sein de – l'Union européenne. En 2003, pendant l'été, le gouvernement italien (tout aussi conservateur que son homologue espagnol) présenta deux projets de loi au sein du troisième pilier : une résolution relative à la sécurité des réunions du Conseil européen et d'autres événements semblables ; et une décision (qui fut finalement convertie en résolution) relative à l'adoption, dans les Etats membres, de l'interdiction d'accès aux enceintes des matches de football revêtant une dimension internationale. Ces mesures furent justifiées comme nécessaires pour contrôler respectivement les manifestations pendant les événements politiques (comme les réunions du Conseil européen ou du G8) et le hooliganisme. Elles introduisent des contrôles renforcés et peuvent donner lieu à l'interdiction d'entrée de certains individus, en fonction de leur « dangerosité », dans le territoire des Etats membres (même dans l'espace Schengen) et dans les stades de football[6]. La résolution sur l'interdiction d'accès aux matches de football fut adoptée en novembre 2003[7], et la plus controversée des résolutions sur la sécurité des réunions fut adoptée.

6 Le projet de loi sur les transporteurs fut justifié, et en fin de compte adopté, en vertu des articles 62(2) (a) et 63(3) (b) du Traité CE. Ces articles servent de fondement légal à l'adoption des mesures relatives respectivement aux contrôles des personnes aux frontières extérieures, et à l'immigration clandestine. De même, l'article 1 du texte finalement adopté[8] spécifie que la directive « *vise à améliorer les contrôles aux frontières et à lutter contre l'immigration clandestine, au moyen de la transmission préalable aux autorités nationales compétentes, par les transporteurs, de données relatives aux passagers* ». Cependant,

comme la directive était non pas l'initiative de la Commission mais d'un Etat membre, elle n'était pas accompagnée d'un mémorandum de justification (*Explanatory Memorandum*) détaillé déclarant les objectifs et comment ceux-ci seraient atteints.

7 Pendant l'examen de la directive par le Comité de l'Union européenne de la Chambre des Lords (*House of Lords European Union Committee*), l'absence de justification détaillée fut soulevée par un certain nombre d'experts, exprimant ainsi des doutes sur l'efficacité du projet[9]. Ce point de vue fut rejeté par le gouvernement britannique, selon lequel la directive renforcerait l'identification des passagers arrivant « sans-papiers » et des passagers voyageant avec des passeports « perdus » ou volés[10]. Le Comité ne fut pas convaincu par cet argument, et nota que la preuve de la nécessité de cette directive n'était pas apportée[11].

8 Malgré le fait que le texte de la directive ait pour objectif de combattre l'immigration clandestine, certains Etats membres ont essayé de présenter cette même directive comme une mesure liée à la sécurité nationale et à la lutte anti-terroriste. Telle était sans doute l'opinion du gouvernement britannique. Mme Caroline Flint, ministre de l'Intérieur en Grande-Bretagne à cette époque, entendue par le *House of Lords EU Committee* (Comité « Union européenne » de la Chambre des Lords), a soutenu que la directive est relative aux contrôles des frontières « *qu'il s'agisse de l'immigration clandestine ou des criminels entrant* [dans le territoire des Etats membres] *ou des individus qui représentent une menace à la sécurité nationale* »[12]. Dans sa réponse au rapport du Comité, la ministre a répété que le gouvernement britannique considère que la directive est nécessaire et justifiée « *pour identifier les menaces migratoires et sécuritaires connues* »[13].

9 L'approche selon laquelle la directive serait une mesure anti-terroriste/liée à la sécurité nationale engendre des doutes quant à la *légalité* de son adoption par le Conseil seulement sous le 1er pilier (droit Communautaire). On peut argumenter que, de la même façon que certaines mesures développent l'acquis Schengen, la transmission des données des passagers (données API) serait justifiée comme une mesure de contrôle frontalier *et aussi* d'anti-terrorisme, nécessitant une double base légale. Cette base légale serait sous le 1er et le 3ème pilier du Traité UE. Cela nécessiterait aussi deux instruments légaux distincts, une directive de « Titre IV » (1er pilier) et une décision cadre du 3ème pilier.

10 L'« encadrement » de la directive comme mesure anti-terroriste/liée à la sécurité nationale avait aussi des conséquences importantes pour l'évaluation de sa *proportionnalité*. La directive fut sévèrement critiquée du fait de la disproportion par rapport à la réussite des objectifs cités : améliorer les contrôles frontaliers et combattre l'immigration clandestine[14]. Toutefois, ces objections apparurent moins fortes dès lors que la directive était justifiée par la nécessité de combattre le terrorisme. L'objectif anti-terroriste pourrait être utilisé pour justifier des mesures intensives – en ce cas, la transmission extensive des données personnelles aux autorités frontalières/ d'immigration. C'était ce point sur la proportionnalité de la directive que Mme Flint a adressé dans sa réponse au Rapport du Comité UE de la Chambre des Lords. Elle notait ainsi que « *la proportionnalité est directement liée à l'objectif de collecte des données* »[15].

11 Ces considérations eurent un effet direct sur les négociations et le *contenu* de la directive, notamment dans le domaine de la protection des données personnelles. L'article 6 de la directive (concernant le traitement des données) fut l'objet de négociations longues et controversées reflétant les approches nationales diverses sur la protection des données transmises sous la directive. Peu avant l'adoption de cette dernière, un accord paraissait

sur l'adoption de standards stricts sur la protection des données, incluant la limitation de l'objectif de transmission (transmission de données pour faciliter les contrôles aux frontières afin de combattre effectivement l'immigration clandestine), des limites aux autorités nationales ayant accès aux données (seulement les autorités frontalières) et la rétention des données (qui seraient effacées par les autorités frontalières dans les 24 heures suivant la transmission et par les transporteurs dans les 24 heures suivant l'arrivée). Toutefois, du fait de la pression exercée par la Grande-Bretagne, deux importantes « concessions » furent accordées :

12 - les données seront effacées par les autorités frontalières dans les 24 heures de la transmission « *à moins qu'elles ne soient nécessaires ultérieurement pour permettre aux autorités chargées d'effectuer les contrôles sur les personnes aux frontières extérieures d'exercer leurs pouvoirs réglementaires conformément au droit national et sous réserve des dispositions relatives à la protection des données figurant dans la directive 95/46/CE* »[16] ;

13 - les Etats membres peuvent utiliser les données transmises « *pour répondre aux besoins des services répressifs* »[17].

14 Il est clair que ces additions rendent les garanties pre-existantes concernant l'accès, la rétention et l'usage de données pratiquement sans intérêt. Il n'est pas du tout surprenant que l'insertion de ces clauses additionnelles ait été saluée par le gouvernement britannique – puisque de cette manière la directive s'alignait sur l'approche britannique « *multi-agency* » associant les contrôles frontaliers et la lutte contre l'immigration clandestine, la criminalité et le terrorisme[18]. Ce lien entre les contrôles d'immigration et les opérations policières est explicite dans l'article 6 de la directive. Cela ne semble pas compatible avec la justification de la directive comme mesure « Titre IV » – visant à renforcer les contrôles frontalières et migratoires. Le lien entre immigration et sécurité nationale est aussi fait dans le préambule de la directive, à un alinéa qui, paradoxalement, semble désigné pour apaiser les préoccupations concernant la protection des données personnelles[19].

15 L'association de la directive aux buts sécuritaires a eu des conséquences considérables du point de vue du déficit démocratique de son examen. En effet, le traitement de cette directive par les Etats ne fut pas du tout satisfaisant. Deux facteurs ont contribué à ce traitement inadéquat. Le premier est lié au fait que la directive n'était pas présentée par la Commission européenne mais par un Etat membre. Selon le traité d'Amsterdam, de tels projets (présentés par des Etats membres) seraient valides seulement jusqu'à cinq ans après la date d'entrée en vigueur dudit traité (1er mai 1999). Donc, si les Etats membres ne parviennent pas à un accord sur le texte au 30 avril 2004, la directive ne peut pas être adoptée. Le deuxième facteur n'est rien d'autre que les attentats de Madrid en mars 2004. Cet évènement a été suivi – presque deux semaines après – par une déclaration du Conseil Européen sur le terrorisme, mettant la priorité sur l'adoption de la directive API.

16 Ces facteurs ont accéléré des procédures d'adoption de la directive, malgré l'opposition du Parlement européen. Selon le Traité CE, le Parlement devrait être consulté avant que la directive ne soit adoptée – mais finalement la directive fut adoptée sans l'avis du Parlement[20]. En Grande-Bretagne, le gouvernement a décidé de passer outre la réserve d'examen parlementaire (*parliamentary scrutiny reserve*) du comité de l'Union européenne de la Chambre des Lords, qui avait exprimé son opposition à la directive. En justifiant cette décision, Mme Flint a évoqué l'urgence post-Madrid d'adopter la directive et les difficultés institutionnelles dans l'UE concernant cette même mesure. Elle a ainsi déclaré :

> « Le Royaume-Uni s'est retrouvé dans une situation doublement difficile à mesure que nous approchions de la fin des négociations. Nous ne disposions pas de l'aval parlementaire pour cette mesure et nous étions le seul Etat membre qui avait encore des réserves importantes sur le texte lui-même. A la lumière de l'urgence nouvelle à approuver la directive, à la suite de la déclaration sur l'anti-terrorisme, nous avons intensifié nos efforts pour obtenir un accord sur les changements que nous considérions vitaux. Nous avons obtenu ces changements au Conseil JAI du mois de mars, grâce au soutien de deux ou trois Etats membres importants et en dépit de la forte opposition d'un autre. Dans le cadre élargi de nos relations européennes cela se serait mal passé si nous avions véritablement bloqué l'adoption de la directive en avril, entraînant sa chute »[21].

17 La directive a ainsi été adoptée le 29 avril 2004, un jour avant l'expiration du délai imparti par le traité d'Amsterdam. Le texte ne requiert plus la transmission des données sur les billets retour et couvre seulement les transporteurs aériens. Mais l'obligation de transmettre les données personnelles des passagers (comme leur nom, leur date de naissance, mais aussi les heures de départ et d'arrivée) aux autorités frontalières demeure – et cette transmission n'est plus réglée par des normes de protection des données aussi strictes. En liant le contrôle des frontières et de l'immigration clandestine à la lutte contre la criminalité et le terrorisme, la directive ouvre la porte à une routinisation de la transmission des données personnelles liées à la vie quotidienne à un nombre considérable d'autorités étatiques, qui peuvent ainsi commencer à construire le profil de tous ceux qui entrent dans l'Union européenne.

18 Réagissant aux attentats du 11 septembre 2001, les Etats-Unis ont adopté une législation en novembre 2001, exigeant que les transporteurs aériens volant aux Etats-Unis, des Etats-Unis ou par les Etats-Unis donnent aux services des *US Customs* un accès électronique aux données inclues dans leurs systèmes automatiques de réservations et de contrôle des départs[22]. Ces données, connues comme « *Passenger Name Records* » (PNR), constituent un dossier où figurent les exigences de chaque passager à propos de son voyage et comporte toute information nécessaire au processus et au contrôle des réservations par les compagnies aériennes. Les données PNR peuvent inclure un grand nombre de détails allant du nom et de l'adresse du passager à son adresse email, en passant par les détails de sa carte bancaire et, même, ses préférences alimentaires pendant le vol. Les données PNR sont donc plus générales que les données API (transmises aux autorités de l'UE suivant la directive déjà analysée). De plus, la législation américaine permet aux *Customs* d'avoir un accès direct aux bases de données des compagnies aériennes (un système « *pull* »), tandis que la directive requiert que les compagnies transmettent les données API aux autorités avant la fin de l'enregistrement (un système « *push* »).

19 La législation américaine est applicable à tous les vols vers les EU, les vols provenant de l'UE inclus. Les compagnies aériennes basées dans l'Union européenne sont donc obligées d'observer ces règles – sans quoi elles seraient soumises à des sanctions pécuniaires considérables et à l'annulation des droits d'atterrissage aux EU. Cependant, l'observation de ces règles pourrait mettre les compagnies en conflit avec le droit communautaire et la législation nationale des Etats membres sur la vie privée et la protection des données personnelles. La Commission européenne a informé les autorités américaines de ce conflit potentiel et le résultat à court terme fut de repousser au 5 mars 2003 l'entrée en vigueur de la législation américaine vis-à-vis des compagnies européennes. Simultanément, la Commission a entamé des négociations avec les autorités américaines dans le but de formuler les normes et les standards rendant les transferts de données PNR compatibles

avec le droit communautaire. Pendant les négociations, le Parlement européen a adopté une série de résolutions conseillant à la Commission d'assurer le respect pour les normes européennes[23]. La législation des EU a aussi été examinée par l'article 29, groupe de protection des données[24], très critique des demandes américaines[25].

20 Les négociations, longues, ont dépassé le délai du 5 mars 2003. Ces négociations aboutirent à un accord entre la Commission et les Etats-Unis le 16 décembre 2003. A la suite d'une série d'actions menées par les autorités américaines, la Commission a accepté, en principe, que la protection des données offerte par les Etats-Unis dans le contexte des transferts PNR était adéquate. La Commission a justifié cette décision par une communication adoptée le même jour, notant que : « *L'option qui aurait consisté, du côté de l'UE, à insister sur le respect du droit communautaire aurait été politiquement justifiée, mais* (...) *aurait ébranlé l'influence de conseils plus modérés et coopératifs à Washington et remplacé par un rapport de force la coopération constructive que nous menons avec notre partenaire* »[26].

21 La Commission a requis une démarche globale de l'Union européenne sur les transferts PNR. Concernant les transferts entre l'UE et les EU, la Commission a proposé comme solution le développement d'un cadre légal réglant les transferts existants de PNR aux Etats-Unis. Ce cadre prendrait la forme d'une décision adoptée par la Commission certifiant la protection adéquate des données PNR par les EU, suivie par un accord international « léger » entre la Communauté européenne et les Etats-Unis.

22 Il est intéressant de noter que, malgré le fait que les lois américaines constituent une réponse législative aux attentats du 11 septembre et soient considérées aux EU comme une mesure anti-terroriste, la Commission (et les Etats membres) ont traité ces demandes comme relatives au fonctionnement propre du marché intérieur (1er pilier) et non pas comme anti-terroristes (appartenant largement au 3ème pilier). Ce choix peut être justifié par les conséquences pratiques et financières de la législation américaine pour les compagnies aériennes, et a servi pour placer la Commission (et pas les Etats membres/la Présidence de l'UE) au coeur des négociations avec les Etats-Unis. En profitant de ce mandat, la Commission a fait des efforts pour consolider cette position centrale de négociateur principal pour l'Union européenne dans ce domaine. Il ne semble pas accidentel que la communication PNR soutienne aussi une démarche européenne globale et la participation européenne aux forums internationaux comme ICAO – où le principal négociateur sera probablement la Commission, et non pas le Conseil ou les Etats membres.

23 Le choix du 1er pilier est important au niveau légal, puisqu'il est le résultat de l'évaluation du caractère adéquat des normes américaines sur la protection des données – et en conséquence la légalité des transferts PNR aux EU – étant faite sous la directive (1er pilier) sur la protection des données de 1995[27]. Selon l'article 25 de la directive, cette évaluation n'est pas faite par le Conseil et le Parlement européen (sous la procédure législative ordinaire de l'UE/co-décision), mais par une « comitologie », c'est-à-dire par un comité composé de représentants des Etats membres, sous la direction de la Commission. La comitologie n'est pas la méthode la plus transparente pour la prise de décisions et laisse un rôle très limité, voire quasi inexistant au Parlement européen et aux parlements nationaux. En Grande-Bretagne, la décision relative à cette évaluation n'a pas été déposée au parlement national, malgré les demandes du Comité de l'Union européenne de la Chambre des Lords[28].

24 La décision sur le caractère adéquat de la protection des données PNR par les Etats-Unis a été examinée par le groupe Article 29[29]. Dans son avis publié en janvier 2004, le groupe a

noté que le progrès fait ne permettait pas une évaluation favorable[30]. Le groupe a justifié cet avis en détaillant une série d'objections sur les règles proposées, et notamment que :

25 - le transfert des données PNR est une exception au principe fondamental (de la protection des données) de la précision de l'objectif de l'usage des données, en vue du nombre et de la sensibilité des données transférées et du nombre de passagers affectés – au moins 10-11 millions par an ;

26 - cela laisse ouverte la possibilité de « *data mining* » et pose le risque de la surveillance généralisée par un Etat tiers ;

27 - la déclaration d'engagement des autorités américaines n'est pas juridiquement contraignante d'un point de vue légal pour les EU – selon le paragraphe 47, la déclaration « *ne crée ni ne confère aucun droit ni aucun avantage pour toute personne ou partie, qu'elle soit privée ou publique* » ;

28 - l'accord conteste le principe de la limitation de l'usage des données – les données PNR peuvent être utilisées pour prévenir et combattre le terrorisme et d'autres crimes graves qui, par nature, revêtent un caractère transnational – la référence aux « autres crimes graves » reste vague et l'objectif de leur utilisation est beaucoup plus étendu que celui de la lutte antiterroriste ;

29 - proportionnalité – les catégories des données transférées sont disproportionnées ;

30 - l'utilisation des données dérivées des données PNR est vague – les données peuvent être utilisées dans des buts anti-terroristes ou policiers légitimes – mais ces buts ne sont pas spécifiés ;

31 - la rétention des données est excessive (3 ans et demi – la demande américaine originale fixait cette détention à 50 ans) ;

32 - les transferts aux autres autorités – l'accord n'inclus pas de liste détaillée des autorités qui peuvent recevoir les données PNR par les *US Customs* ;

33 - il est nécessaire de remplacer le système « *pull* » par un système « *push* » selon lequel ce sont les compagnies aériennes qui transfèrent les données aux autorités américaines[31].

34 Malgré son rôle limité sous la procédure de la comitologie, le Parlement européen a adopté, le 30 mars 2004, une résolution – un appel pour que la Commission retire la décision certifiant que la protection des données PNR aux EU est adéquate[32]. Le Parlement a réitéré plusieurs des préoccupations sur la protection des données déjà analysées et a noté, à propos de la légalité, qu'il n'existe pas en droit communautaire de base légale permettant l'usage des données commerciales PNR pour des objectifs de sécurité publique – une base légale spécifique est nécessaire, selon le Parlement, pour ces cas. La décision peut faire baisser le niveau de la protection des données personnelles établi par la directive de 1995.

35 Le Parlement a également demandé un avis de la Cour de Justice au Luxembourg sur la compatibilité de l'accord international PNR (qui suivrait l'adoption de la décision) et du traité CE. Le Parlement attendrait la réponse avant de transmettre son avis sur l'accord au Conseil suivant la procédure de consultation de l'Article 300 TCE. Le Conseil a imposé le délai du 22 avril 2004 pour la transmission de l'avis parlementaire, délai repoussé au 5 mai[33]. En attendant la réaction de la Cour, le Conseil a décidé de procéder à la conclusion de l'accord international sans avoir reçu l'avis du Parlement, justifiant ce choix par la nécessité urgente de remédier à la situation d'incertitude pour les compagnies aériennes et les passagers (décision autorisant l'accord, préambule alinéa 2).

36 En Grande-Bretagne, le Parlement fut également écarté. Comme dans le cas de la directive API, le gouvernement britannique a décidé de passer outre la réserve d'examen parlementaire (*parliamentary scrutiny reserve*) du Comité de l'Union européenne de la Chambre des Lords. Lord Filkin, ministre au *Department for Constitutionnal Affairs*, a justifié cette décision en adoptant des arguments similaires à ceux de la Commission. Il a aussi mis l'accent sur l'importance de cet accord pour la « guerre contre le terrorisme », notant que :

37 « l'Union européenne a récemment réaffirmé son engagement dans la lutte anti-terroriste au vu des terribles évènements de Madrid en mars. L'UE et les Etats-Unis sont en parfait accord sur ce point. La présente proposition offre la possibilité de montrer notre engagement. Nous devons en effet faire très attention au message que nous ferons passer si nous refusons cet accord »[34].

38 La décision de la Commission a finalement été adoptée le 14 mai 2004[35]. Elle a été suivie, trois jours après, par une décision du Conseil autorisant le président du Conseil à signer pour la Communauté européenne l'accord PNR avec les Etats-Unis[36]. Le texte de l'accord et celui de la déclaration d'engagement sont identiques aux textes examinés – et rejetés – par le groupe de l'Article 29 et le Parlement européen. Selon ces textes :

39 - 34 catégories de données PNR sont demandées par les *US Customs* – parmi lesquelles le nom, l'adresse et l'adresse de facturation, l'adresse électronique, des informations sur les modes de paiement, l'itinéraire complet, des informations sur les « grands voyageurs », sur le « statut » du voyageur, des informations sur les passagers répertoriés comme défaillants et les passagers de dernière minute sans réservation, les allers simples, l'historique des changements au PNR et des « observations générales » ;

40 - le CBP (*Customs*) « extraira » les informations PNR des systèmes de réservation des compagnies aériennes jusqu'à ce que celles-ci soient en mesure de mettre en oeuvre un système « exportant » les données concernées vers le CBP[37] ;

41 - le CBP utilise les données PNR dans le but unique de prévenir et de combattre le terrorisme et les crimes liés au terrorisme, et tout autres crimes graves qui, par nature, revêtent un caractère transnational[38] ;

42 - la rétention des données PNR durera 3 ans et six mois. Les données qui n'auront pas été consultées manuellement durant ce laps de temps seront détruites. Les données consultées seront conservées pour une période additionnelle de 8 ans. Ces délais ne s'appliqueraient toutefois pas aux données PNR en rapport avec un dossier spécifique[39] ;

43 - le CBP peut transmettre les données PNR à d'autres autorités gouvernementales de répression ou de lutte contre le terrorisme, qu'elles soient nationales ou étrangères, qu'au cas par cas, pour prévenir et combattre le terrorisme et la criminalité transnationale grave [40] ;

44 - dans l'éventualité où serait mis en oeuvre un système de transmission de PNR par l'UE, le CBP s'engage à « encourager », à titre de réciprocité, les compagnies aériennes établies aux Etats-Unis à coopérer [41] ;

45 - la déclaration d'engagement est applicable pendant une période de trois ans et demi et peut être étendue[42] ;

46 - la déclaration ne créée ni ne confère aucun droit ni avantage à toute personne ou partie, qu'elle soit privée ou publique. Elle ne constitue aucun précédent pour toute discussion ultérieure avec la Commission, l'UE et les organisations/Etats tiers[43].

47 Aucune des préoccupations du groupe article 29 ne fut abordée. Le système de transmission des données PNR couvre des catégories très étendues de données personnelles et renforce l'argument du groupe selon lequel cette transmission constitue la surveillance généralisée par un Etat tiers et participe à la construction de profils d'individus. Les demandes de la législation américaine sont disproportionnées et semblent être contraires aux droits fondamentaux relatifs à la vie privée et à la protection des données personnelles bien établis dans le droit communautaire. La Commission a mis l'accent sur les concessions obtenues des Américains, mais la force légale des engagements est douteuse. Les préoccupations sur la protection de la vie privée et des données personnelles sont renforcées par le fait que l'accord permet la transmission de PNR provenant de l'UE par les autorités américaines aux pays tiers – laissant ainsi en effet les autorités américaines seules juges de l'adéquation de la protection des droits de l'Homme offerte par ces pays. Le Parlement européen a demandé l'annulation de la décision autorisant la conclusion de l'accord entre l'UE et les Etats-Unis [44]. Le jugement de la Cour est attendu avec intérêt.

48 Les négociations entre la Commission et les Etats-Unis présentent, comme en d'autres occasions, le dilemme de la coopération de l'Union européenne avec des pays tiers au risque de compromettre le droit et les valeurs de l'UE[45]. Dans le cas du PNR, la Commission a saisi l'opportunité de représenter les Etats membres (en considérant les échanges PNR comme une question relative au marché intérieur/1er pilier) et peut prétendre que l'accord UE/EU n'est pas inégal, puisque les engagements américains contiennent une clause de réciprocité. Cette clause est cependant conditionnelle à la mise en place par l'Union européenne d'un système de transmission des données PNR identique au modèle américain. Cela peut anticiper la décision par les institutions européens rendant un tel système souhaitable dans l'Union européenne (ou même compatible avec le droit communautaire et les droits fondamentaux). Même si un tel système est mis en place dans l'UE, l'engagement américain stipule uniquement que les *US Customs* « encourageront » les compagnies aériennes établies aux EU à coopérer[46].

49 Dans le cas des PNR, entre autres, la légitimité de la position des négociateurs européens, et l'accord ultimement accepté, furent ébranlés par l'absence de transparence et l'absence d'examen significatif et détaillé des questions par le Parlement européen et les parlements nationaux des Etats membres. Il est regrettable que les institutions européennes aient choisi de procéder à l'adoption de la décision relative à la protection adéquate les données par les EU et à la signature de l'accord autorisant les transferts PNR dans un délai limité, malgré l'opposition expresse du Parlement européen et des parlements nationaux et l'avis critique du groupe (de la protection des données) de l'article 29. C'est encore un exemple de décisions prises sous une pression « fabriquée » par un discours d'urgence. Comme dans le cas des mesures de l'UE adoptées post 11 septembre (telles que le mandat d'arrêt européen), cette perception de « l'état d'urgence » a été utilisée pour accélérer l'adoption d'une législation d'une portée considérable en minimisant l'examen démocratique et en marginalisant ainsi les objections « gênantes » présentées par les parlements et la société civile. La Commission présentera, en 2005, des projets de loi concernant une démarche commune de l'UE pour le transfert des données PNR – on espère que ces projets feront l'objet d'un dialogue ouvert et d'un examen parlementaire étendu, afin d'assurer que la coopération mondiale dans ce domaine ne menace et ne compromette pas les principes fondamentaux du droit communautaire et des droits nationaux. Il reste à voir si la voix de l'Union européenne est

suffisamment forte au niveau global pour soutenir ces principes et les promouvoir dans un esprit de « réciprocité ».

50 La réponse américaine au 11 septembre, ayant la « sécurité frontalière » comme pilier central, a été largement suivie par les chefs d'Etats de l'Union européenne suite aux attentats de Madrid. La déclaration du Conseil européen du 25 mars 2004 sur la lutte anti-terroriste a lié les contrôles des mouvements des personnes à la « guerre au terrorisme », en notant que l'amélioration des contrôles des frontières et de la sécurité des documents joue un rôle important dans la lutte anti-terroriste. Cette démarche est composée de deux éléments : l'inclusion des indicateurs biométriques aux visas et passeports européens qui devrait être rendue prioritaire et suivie de mesures adoptées avant la fin de l'année 2004 ; ainsi que l'interopérabilité entre les bases de données européennes et la création de « synergies » entre les systèmes d'information existants et ceux à venir (comme SIS II, VIS et Eurodac). Selon le Conseil européen, cette interopérabilité est nécessaire pour exploiter la « valeur ajoutée » dans les cadres techniques et législatifs de ces bases de données pour prévenir et combattre le terrorisme.

51 Aucune de ces idées ne serait neuve. On a vu une intensification des débats ainsi qu'une pression politique au sein des institutions européennes sur la nécessité d'une réponse de l'UE au 11 septembre. Au conseil informel des ministres JAI à Veria (28/29 mars 2003), le Conseil a invité la Commission à présenter un projet de loi afin d'intégrer les identificateurs biométriques aux visas. Le membre de la Commission responsable du JAI à cette époque, Antonio Vitorino, a aussi soutenu l'inclusion des identificateurs biométriques aux passeports des Etats membres. Selon la Commission, cela était nécessaire parce que l'UE devrait adopter une démarche commune vis-à-vis de la législation américaine exigeant l'inclusion d'identificateurs biométriques aux passeports des pays bénéficiaires par un programme de « *visa waiver* » dès le 26 octobre 2004. Quelques mois après le conseil à Thessalonique, le Conseil européen des 19 et 20 juin a soutenu une démarche cohérente de l'Union européenne sur la biométrie, qui aboutirait à des solutions harmonisées pour les documents des citoyens des pays tiers, les passeports des citoyens de l'Union et les systèmes d'information (SIS II, VIS). Le Conseil a invité la Commission à présenter des projets de lois similaires[47].

52 La Commission – et en suite le Conseil des ministres et le Conseil européen – ont donc évoqué encore une fois les demandes américaines pour légitimer l'action de l'Union européenne dans un domaine contesté – et pour étendre ce domaine d'action à l'inclusion de mesures relatives au contenu des passeports des citoyens de l'UE. En mars 2004 (au moment des attentats à Madrid qui ont donné lieu à l'utilisation de la notion de « guerre au terrorisme » comme facteur additionnel de légitimité pour l'action de l'Union européenne dans ce domaine), des négociations au Conseil concernant l'inclusion des identificateurs biométriques aux passeports étaient déjà avancées. Ces développements ont eu lieu malgré les objections du groupe article 29 qui avait exprimé sa préoccupation sur la capacité de l'usage extensif de données biométriques à « désensibiliser » le public sur l'effet potentiel de cette utilisation sur la vie quotidienne. Le groupe a mis les institutions européennes en garde contre l'utilisation des identificateurs biométriques qui peuvent laisser des traces physiques (comme les empreintes digitales) ou qui peuvent être mémorisés[48].

53 Le Programme de la Haye, adopté par le Conseil européen les 4 et 5 novembre 2004, a maintenu l'élan pour l'inclusion des identificateurs biométriques en répétant, de façon

plus claire, le lien entre le mouvement, l'immigration et le terrorisme. La première partie du paragraphe 1.7.2 stipule :

54 « La gestion des flux migratoires, y compris la lutte contre l'immigration clandestine, devrait être renforcée par la mise en place d'un ensemble de mesures de sécurité reliant efficacement les procédures de demande de visa et les procédures d'entrée et de sortie lors du franchissement des frontières extérieures. Ces mesures revêtent également de l'importance pour la prévention et la répression de la criminalité, en particulier du terrorisme. A cette fin, l'UE doit adopter une approche cohérente et des solutions harmonisées concernant les identificateurs et les données biométriques »[49].

55 Le concept du « continuum de l'(in)sécurité » dans l'Union européenne (où les questions relatives à l'immigration sont liées, dans le discours politique/policier, avec la lutte contre la criminalité et le terrorisme), qui a été introduit par les théoriciens comme une réponse au développement des politiques européennes sur la justice et les affaires intérieures des années 1990[50] apparaît donc au coeur d'un document officiel important de l'Union européenne – le programme de long terme de l'action européenne sur JAI.

56 Alors que le terme avait été introduit pour mettre en garde contre les dangers pour les libertés civiles d'une problématique seulement axée sur la discrimination et la répression, le continuum de sécurité apparaît dans le programme de la Haye comme un phénomène légitime, comme une réponse nécessaire au monde post-11 septembre. Les contrôles du mouvement, de la criminalité et du terrorisme fusionnent. Ces contrôles deviennent encore plus une priorité et sont approfondis par l'usage de mesures constituant une intrusion maximale dans la sphère individuelle – des identificateurs biométriques.

57 La pression politique en vue de l'insertion des identificateurs biométriques aux documents d'identité a donné lieu à l'adoption, en décembre 2004, d'un règlement du Conseil introduisant de tels identificateurs (sous la forme de photos du visage et d'empreintes digitales) aux passeports des Etats membres de l'Union européenne[51]. Comme dans le cas de la directive API, le fondement légal du règlement est l'article 62(2) (a) du traité CE sur le contrôle des frontières extérieures. Dans ce cas également le règlement était justifié comme mesure sécuritaire[52]. Ledit règlement a été adopté malgré les importantes objections concernant le fondement légal et l'existence de la compétence permettant à la Communauté européenne d'adopter une législation contraignante sur le contenu des documents d'identité. Les mesures européennes pré-existantes dans ce domaine étaient des résolutions (qui n'ont pas la force légale d'un règlement). L'article 62 (2) (a) fait référence aux contrôles des frontières extérieures de l'Union européenne, et non pas au contenu des documents de voyage. Aussi, l'article 18(3) du traité CE (sur la citoyenneté européenne) stipule expressément que l'action communautaire pour faciliter l'exercice des droits de la citoyenneté n'est pas applicable aux règles concernant les passeports, les cartes d'identité ou autres documents du même genre[53]. Malgré ces objections sur la légalité, et les préoccupations sur sa proportionnalité[54], les négociations sur le règlement ont avancé rapidement et un deuxième identificateur – les empreintes digitales – a été ajouté au dernier moment. Malgré les objections du groupe article 29[55], le règlement a été adopté rapidement (en décembre 2004) – peut-être pour éviter les objections du Parlement européen, devenu co-législateur (avec le Conseil) ayant droit de veto sur ce domaine dès le 1er janvier 2005[56]. Certains travaux sur la biométrie des visas et des cartes de résidence sont aussi en Cours, malgré une série de problèmes techniques.

58 Les identificateurs biométriques auront de la valeur pour les autorités policières pour autant qu'ils seront facilement accessibles au sein des bases de données. Il n'est donc pas

surprenant que dans l'Union européenne, comme aux Etats-Unis, les appels en faveur de l'utilisation des identificateurs biométriques soient accompagnés d'appels pour faciliter leur inclusion aux bases de données et pour faciliter l'« interopérabilité » de ces bases de données. Il faut rappeler ici que l'utilisation de la biométrie et l'interopérabilité des bases de données ont été à de nombreuses occasions associées par le Conseil européen, et plus récemment dans le programme de la Haye. La Commission développe, depuis quelques années, le système d'information Schengen « deuxième génération » (SIS II). L'objectif est ici de rendre possible l'inclusion à SIS II de quantités de données plus importantes et de données plus détaillées (incluant les identificateurs biométriques). L'autre objectif central est de faciliter les « synergies » entre SIS II et d'autres systèmes comme le système d'information sur les visas (VIS). L'importance de ce projet pour la Commission est révélée par la création d'un nouveau bureau, responsable des systèmes d'information de grande ampleur, au sein de DG JAI, le 16 décembre 2002[57].

59 Les travaux sur le développement du SIS II et de l'un de ses « interlocuteurs principaux », VIS, se poursuivent. Le Conseil JAI a adopté les conclusions détaillées sur le développement du VIS en février 2004, notant qu'un des objectifs du VIS était de contribuer à l'amélioration de l'administration de la politique commune sur les visas, sur la sécurité intérieure et sur la lutte contre le terrorisme. Le Conseil a soutenu l'inclusion des identificateurs biométriques des demandeurs de visas au VIS afin de vérifier et d'identifier ces personnes (les vérifications des antécédents des individus « *background checks* » inclus). Le Conseil a aussi soutenu l'autorisation d'accès au VIS *inter alia* par les gardes-frontières et autres autorités nationales, comme les services policiers, les services d'immigration et les services responsables de la sécurité intérieure. C'est un autre exemple du « continuum de la sécurité » dans le discours politique de l'Union européenne...

60 Le Conseil a adopté en juin 2004 une décision formant la base légale à l'établissement du VIS[58], et des négociations ont commencé pour définir l'objectif et les fonctions du système ainsi que pour formuler des règles précises sur l'accès et l'échange des données. Suite à cela, le groupe d'article 29 a publié un avis très critique sur cette initiative. Le groupe a rappelé ses préoccupations sur le traitement des données biométriques dans le VIS et sur la proportionnalité du stockage de ces données pour effectuer les contrôles postérieurs des immigrés clandestins (ces contrôles étaient apparemment envisagés comme un objectif du VIS par le Conseil JAI). Le groupe a noté que les normes de la directive sur la protection des données de 1995 ne peuvent être contournées par l'introduction d'objectifs étendus et multiples. Le groupe a également exprimé ses préoccupations sur la proportionnalité de l'inclusion des identificateurs biométriques et sur le VIS lui-même, notant que certains objectifs du VIS recoupaient ceux du SIS II. Le groupe a demandé l'examen détaillé des projets sur l'interopérabilité entre ces systèmes[59].

61 La Commission a récemment présenté un règlement ayant pour but d'amener le VIS encore plus loin par la définition de ses objectifs et l'établissement des règles relatives à l'accès et à l'échange des données[60]. Le projet du règlement est le résultat d'une consultation extensive et la Commission a fait des efforts considérables pour contrebalancer le choix d'une forme d'intervention très envahissante (l'usage de la biométrie dans le VIS) en limitant l'accès au VIS et en incluant au texte des garanties détaillées sur la protection des données ainsi qu'un article de « proportionnalité », selon lequel les données biométriques ne seront pas stockées dans le VIS. Toutefois, on peut encore distinguer dans le règlement la logique du « continuum de la sécurité » : l'article 1

(2) (a) note qu'un des objectifs du VIS est de prévenir les menaces à la sécurité intérieure des Etats membres. De plus, les conclusions du récent Conseil JAI du 24 février provoquent l'inquiétude selon laquelle les garanties introduites par la Commission seront démontées par les Etats membres pendant les négociations au Conseil. Le Conseil soutient l'accès au VIS des autorités nationales responsables de « la sécurité intérieure », quand celles-ci exercent leurs pouvoirs d'investigation, de prévention et de détection des crimes (y compris les actes et les « menaces » terroristes). Le Conseil a invité la Commission à présenter un projet de loi séparé (du 3ème pilier) dans ce but. Ce développement renforce la logique du « continuum de la sécurité », mais marginalise aussi effectivement le Parlement européen. Le Parlement a un rôle de co-décision avec le Conseil sur le règlement du 1er pilier présenté par la Commission, mais il sera seulement consulté sur le projet de loi du 3ème pilier.

62 Sous le drapeau de l'« interopérabilité », on avance donc vers un système dans lequel les bases de données de l'Union européenne contenant d'importants volumes de données personnelles sensibles peuvent être interconnectés et accessibles à un nombre considérable d'agences étatiques. Ce développement est rendu possible en dépit du fait que les bases de données européennes aient été construites dans des objectifs très divers – de la facilitation de l'examen des demandes de visas et d'asile (VIS, Eurodac) à la coopération policière et à l'anti-terrorisme (aspects du SIS, Europol) – et en dépit du fait qu'elles contiennent des catégories de données variées. Ainsi, l'interopérabilité – notamment si elle est justifiée par la logique de la « guerre anti-terroriste » – peut rendre les garanties sur l'accès et l'utilisation de ces bases de données dépourvues de sens et d'effet.

63 Cette complexité est encore plus forte du fait que les bases de données européennes, à cause de leur diversité, ont été établies sous des bases légales différentes (1er/3ème piliers) et sont réglées par des régimes de protection des données différents. Ces régimes sont très fragmentaires dans le 3ème pilier, où les règles et les systèmes de supervision spécifiques sont applicables pour chaque agence spécifiques (comme Eurojust et Europol) – il n'y a donc pas de cadre commun de législation et de supervision de la protection des données dans le 3ème pilier. Ces garanties fragmentaires paraissent limitées et inefficaces dans un climat où l'accès maximum aux données personnelles est facilité, et la coopération opérationnelle entre les agences de contrôle au niveau européen[61] – mais aussi au niveau national (y compris la coopération entre la police et les services de renseignements) – est l'élément central de l'action de l'Union européenne dans le domaine de la Justice et des Affaires Intérieures pour les cinq prochaines années[62].

64 Cette analyse peint un sombre tableau de la renégociation de la relation entre l'individu et l'Etat, en Europe et au niveau mondial, à propos du contrôle étatique sur la vie privée. La surveillance étatique s'étend et s'approfondie. Les données personnelles sont rassemblées sur toute la population, et pas seulement sur des catégories spécifiques d'individus suspects – et la surveillance passe ainsi d'une surveillance spécifique à une surveillance généralisée. D'importants volumes de données sont rassemblés par une variété de sources, afin de créer un profil des individus et de tracer leur mouvement autour du globe. L'arrivée des personnes (et leur départ) dans les territoires nationaux des Etats membres de l'UE (et dans l'espace Schengen) est surveillée et enregistrée. Les données sont assemblées avant, pendant et après l'entrée dans le territoire. La nature des données assemblées a également changé – l'Etat envahit la sphère privée en assemblant les données inséparables de l'essence de l'identité personnelle et de l'humanité : les

identificateurs biométriques. La transmission des données, originellement « réactive » (les compagnies privées répondant aux demandes policières concernant les suspects spécifiques) est devenue largement « proactive » – par exemple, les compagnies aériennes sont obligées de transmettre les données sur tous les passagers aux autorités. Cela résulte de ce qu'Ericson et Haggerty ont appelé « *the disappearance of the disappearance* » (la disparition de la disparition), un processus dans lequel « *il est plus et plus difficile pour les individus de garder leur anonymat ou d'échapper aux contrôles des situations sociales* »[63] – en ce cas d'être happé par l'Etat assisté par le secteur privé[64].

65 Cette intensification massive de la surveillance a été légitimisée par « la guerre contre le terrorisme ». Les gouvernements et les législateurs prétendent que depuis le 11 septembre, tout est lié dans un « continuum de sécurité ». Il faut contrôler de la même façon l'immigration, la criminalité et le terrorisme, puisque ces phénomènes – et leur contrôle – sont associés. Cette vision du monde pose des questions fondamentales concernant la criminalisation des immigrés et la dénomination de l'« Autre »[65]. En même temps, le « continuum sécuritaire » représente un défi considérable pour les principes légaux bien fondés et pour les droits fondamentaux. Dans le climat actuel de « continuum sécuritaire », il est très difficile de présenter des garanties pour la protection des données et ainsi du droit à la vie privée et à l'identité. L'accès par l'Etat aux données non policières est justifié (et considéré comme proportionnel) « afin de combattre le terrorisme » (un des nombreux exemples où la « guerre anti-terroriste » est évoquée pour changer ou ignorer la légalité et les droits fondamentaux). Cette logique de la guerre justifie aussi l'interopérabilité des bases de données, même si ces bases de données servent des fins différentes et contiennent des données différentes – toutes ces données pourraient aider à la « guerre anti-terroriste ». C'est pourquoi, selon le discours politique, il est nécessaire de permettre aux autorités policières d'accéder à ces bases de données – même ces dernières ne contiennent pas d'informations liées à la criminalité. Dans de telles circonstances, comment peut-on parler du respect de la « limitation des fins » de l'usage des données personnelles ?

66 Ces développements soulèvent aussi une série de paradoxes pour l'Union européenne et ses Etats membres. Le premier paradoxe concerne la relation entre l'objectif de construction d'une Union européenne sans frontières et sans contrôles à l'intérieur, et l'intensification des contrôles et de la surveillance de l'autre côté. Le deuxième paradoxe concerne la coexistence d'une pression pour créer une identité européenne fondée sur la légalité et la protection des droits fondamentaux, et l'évocation de cette identité par rapport aux relations extérieures de l'Union européenne négociant par « une voix », avec la résignation des institutions européennes de compromettre ces principes quand ils parlent d'« une voix » lors de négociations internationales. Le troisième paradoxe concerne la question de savoir si l'Union européenne elle-même peut protéger et promouvoir les droits de l'Homme à une époque où on a peur de prendre des décisions démocratiques et transparentes, quand en même temps les Etats membres abaissent le niveau de la protection des droits de l'Homme et essayent de limiter l'examen démocratique des projets de loi sécuritaires.

67 Ces paradoxes semblent difficiles à résoudre, mais il reste un espace pour l'optimisme dans le futur. Le programme de la Haye met l'accent sur la surveillance et l'interopérabilité, mais il contient aussi un appel pour le développement d'un cadre légal pour la protection des données dans le 3ème pilier. Bien que ce développement n'ait pas abordé le caractère fragmentaire des politiques européennes divisées entre les piliers, ce

cadre est une opportunité pour les Etats membres de réexaminer les règles existantes limitées et de développer des règles véritablement protectrices, qui aborderont le caractère intensif et étendu de l'assemblage des données et de la surveillance. Les règles présentes sont trop fragmentaires pour répondre au « *profiling* » généralisé des individus. Il faut examiner comment protéger la vie privée effectivement en vue de ces développements et s'il est nécessaire de donner aux autorités chargées de la supervision de la protection des données au niveau national, communautaire et européen des pouvoirs plus étendus et un rôle plus grand au développement de la loi et des politiques concernant la vie privée.

68 La Constitution européenne peut être un catalyseur de davantage de protection des droits fondamentaux. La Constitution incorpore dans son texte (dans la partie II) la Charte européenne des droits fondamentaux – qui inclut un droit à la protection des données – et supprime les piliers. Cela peut donner lieu à une interprétation plus « expresse » du droit européen par la Cour de Justice à la lumière des droits à la vie privée et à la protection des données, et l'obligation de l'Union de protéger et de respecter les droits fondamentaux (notamment concernant ses relations extérieures, par lesquels la Constitution pourrait aussi donner lieu au développement d'une voix commune à l'UE plus forte). La Constitution rend aussi l'adoption de la législation aux domaines examinés ici plus transparente et démocratique, et augmente l'influence des voix qui, jusqu'à présent, sont dissidentes mais ignorées (comme le Parlement Européen et les parlements nationaux). Quel que soit l'avenir de la Constitution, il est essentiel d'adopter des lois plus démocratiques et de faciliter la participation du public si l'action de l'Union européenne dans le domaine sécuritaire se veut légitime.

NOTES

1.

2.1. Nous souhaiterions remercier Didier Bigo et la rédaction de *Cultures & Conflits* pour leurs lectures et commentaires utiles sur ce texte.

. JO C 82, 5.4.2003, p. 23.

3.. *Ibid.* Pour une analyse détaillée, voir House of Lords EU Committee, *Fighting Illegal Immigration: Should Carriers Carry the Burden?*, 5th Report, session 2003-04, HL Paper 29.

4.. Communication de la Commission au Parlement européen et au Conseil en vue du Conseil européen de Thessalonique sur le développement d'une politique commune en matière d'immigration clandestine, de trafic illicite et de traite des êtres humains, de frontières extérieures et de retour des personnes en séjour irrégulier, COM (2003) 323 final, Bruxelles, 3 juin 2003.

5.. *Ibid.*

6.. Les contrôles sur la sécurité des réunions s'ajoutent au pouvoir qu'ont les Etats-Schengen de réintroduire des contrôles aux frontières en cas d'urgence (Article 2(2) de la Convention Schengen). On peut ainsi passer de contrôles exceptionnels mais généralisés à

tous les individus, à la normalisation des contrôles pour des individus spécifiques selon une analyse du risque spécifique.

7.. JO C281, 22 novembre 2003, p. 1.

8.. Directive 2004/82/CE du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, JO L261, 6.8.2004, p. 24.

9.. Voir notamment ILPA (Immigration Law Practitioners' Association), *Fighting Illegal Immigration* – note 2.

10.. *Ibid*.

11.. *Ibid*, paragraphe 10.

12.. *Ibid*., paragraphe 9.

13.. Lettre en date du 1er avril 2004, reproduite par le House of Lords EU Committee, *Government Responses*, 26th Report, Session 2003-04, HL Paper 164, p. 13.

14.. Voir *House of Lords*, note 2, pp. 8-9.

15.. Lettre en date du 1er avril 2004, voir note 13.

16.. Article 6(1). Voir le document du Conseil 7595/04, Bruxelles, 23 mars 2004, introduisant ces concessions.

17.. *Ibid*.

18.. Voir la lettre de Mme Flint du 1er avril 2004, note 13. Voir aussi la stratégie britannique sur les contrôles des frontières – *Home Office*, *Five Year Strategy for Asylum and Immigration* (Cm 6472). Le gouvernement veut introduire la législation rendant possible l'échange des données personnelles entre le *Immigration Service*, *HM Customs* et la police (paragraphe 58). La coopération entre les agences diverses est aussi soulignée dans le contexte du développement du programme « e-borders » (annexe 1).

19.. Alinéa 12, qui note que le traitement des données serait légitime « également dans le but de permettre l'utilisation de ces données comme élément de preuve dans des procédures visant à l'application des lois et des règlements sur l'entrée et l'immigration, notamment des dispositions relatives à la protection de l'ordre public et de la sécurité nationale... ».

20.. Voir le préambule de la directive, notamment les alinéas 2-6. Selon la directive, « le Conseil a épuisé toutes les possibilités d'obtenir l'avis du Parlement européen dans les délais » et « étant donné ces circonstances exceptionnelles, il convient d'adopter la directive en l'absence de l'avis du Parlement », (alinéas 5 et 6).

21.. Lettre à Lord Grenfell, 11 mai 2004, publiée par le House of Lords EU Committee, *Correspondence with Ministers*, 25th Report, 2003-04, HL Paper 140.

22.. Titre 49, US Code, section 44909(c)(3) et titre 19, Code of Federal Regulations, section 122.49b. Sur la réponse des européens concernant la sécurité des frontières voir Ceyhan A., « Sécurité, frontières et surveillance aux Etats-Unis après le 11 septembre 2001 », *Cultures & Conflits*, L'Harmattan, n°53, pp. 113-145.

23.. Voir la Résolution P5_TA(2003)0097 et P5_TA(2003)0429.

24.. Etabli par la directive de 1995 sur la protection des données (Article 29) et composé des chefs des autorités nationales pour la protection des données. Le groupe a un rôle de conseiller.

25.. Avis 4/2003 sur le niveau de protection assuré aux Etats-Unis pour le transfert des données des passagers, doc. 11070/03, WP 78. Le groupe a conseillé à la Commission d'assurer *inter alia* que les objectifs de transfert des données et les autorités ayant accès à ces données soient specifiés et le principe de la proportionnalité respecté.

26.. Communication de la Commission au Conseil et au Parlement, *Transfert des données des dossiers passagers (Passenger Name Record –PNR) : Une démarche globale de l'Union européenne*, COM (2003) 826 final, Bruxelles, le 16 décembre 2003, p. 6.
27.. JO L281, 23 novembre 1995, p. 31.
28.. Voir la lettre du 12 février 2004 par Lord Grenfell et la réponse du ministre compétent, Lord Filkin de 26 février 2004 – selon lequel le gouvernement britannique n'a pas identifié la décision comme étant assez importante pour être déposée exceptionnellement au Parlement) – reproduites par le House of Lords EU Committee, *Corespondence with Ministers,* note 20.
29.. Le groupe a pour mandat d'examiner de telles décisions sous l'article 30(1)(b) de la directive de 1995.
30.. Avis 2/2004, doc. 10019/04, WP 87.
31.. *Ibid*. Voir aussi l'examen du House of Lords EU Committee, en particulier la lettre de Lord Grenfell du 12 février 2004, voir note 20.
32.. P5_TA-PROV (2004)0245.
33.. Lettre de Lord Filkin à Lord Grenfell du 27 avril 2004, voir note 20.
34.. Lettre à Lord Grenfell du 11 mai 2004, reproduite par le House of Lords EU Committee, *Correspondence with Ministers,* note 20. Voir aussi sa lettre du 27 avril, dans laquelle Lord Filkin note que les Etats-Unis offrent un niveau de protection des données adéquat et, que « *même si tel n'était pas le cas, les transferts ne seraient pas forcément illégaux* ». *Ibid*.
35.. JO L235, 6.7.2004, p. 11. La Déclaration d'engagement du *EU Homeland Security Department* est aussi reproduite (pp. 15-21). Pour une liste des données PNR, voir p. 22.
36.. JO L183, 20 mai 2004, p. 83. Pour le texte de l'accord, voir pp. 84-85. L'accord a été signé le 28 mai 2004.
37.. Engagement 13. Il n'est pas évident de savoir comment on va garantir la légalité de cette « extraction » et assurer que ladite « extraction » ne concerne que des données des passagers des vols aux Etats-Unis (et n'est pas une « extraction » généralisée).
38.. Engagement 3.
39.. Engagement 15.
40.. Engagement 29.
41.. Engagement 45.
42.. Engagement 46.
43.. Engagements 47 et 48.
44.. Le Parlement considère que l'article 95 du Traité CE (sur le marché intérieur) n'est pas la base légale qui convient pour la décision. Toujours selon lui, la procédure correcte pour l'adoption de la décision requiert l'approbation du Parlement et pas seulement sa consultation parce que, selon le Parlement, la décision constitue en effet une modification de la directive de 1995. Voir le document du Conseil 11876/04, 6 août 2004.
45.. Voir Mitsilegas V., « The New EU/US Co-operation on Extradition, Mutual Legal Assistance and the Exchange of Police Data », *European Foreign Affairs Review*, 8/4, 2003, p. 515.
46.. Engagement 45.
47.. Voir les explications accompagnant le projet de règlement présenté par la Commission modifiant le format uniforme pour les visas, COM (2003) 558 final, Bruxelles, 24 septembre 2003.
48.. Document de travail sur les identificateurs biométriques, 1er août 2003, doc. 12168/02 WP 80.

49.. La version anglaise d'« un ensemble de mesures » est « *security continuum* ».
50.. Voir les travaux de Didier Bigo, notamment *Polices en Réseaux : l'experience européenne*, Paris, Presses de Sciences Po, 1996.
51.. Règlement 2252/2004, JO L 385, 29 décembre 2004, p. 1.
52.. Voir la lettre du 15 juillet 2004 de Mme Caroline Flint à Lord Grenfell, président du House of Lors EU Committee, stipulant « nous considérons que la proposition actuelle est avant tout une mesure sécuritaire », nous traduisons.
53.. Voir les travaux du House of Lords EU Committee, en particulier la lettre du 21 octobre 2004 de Lord Grenfell à Caroline Flint. Le gouvernement britannique, originellement opposé au choix de la base légale, l'a finalement soutenu en affirmant que les règles communes au niveau européen faciliteraient les contrôles frontaliers parce que l'équipe de vérification des documents aux frontières devrait être capable de lire électroniquement les données des passeports de l'UE (voir la lettre du 15 juillet de Caroline Flint à Lord Grenfell). Ironiquement, la Grande-Bretagne a été exclue de sa participation au règlement par les pays Schengen.
54.. Voir l'analyse suivante par Statewatch, preparée par Steve Peers : *The Legality of the Regulation on EU Citizens' Passports*, 26 novembre 2004, www.statewatch.org.
55.. Lettre du 30 novembre 2004 de Peter Schaar, président du groupe, à Josep Borrell Fontelles, président du Parlement européen. Le groupe a exprimé ses préoccupations concernant l'usage de « *données biométriques telles que les empreintes digitales permettant une identification et un traçage 'de trop' des individus* ». Le groupe a demandé le respect du droit fondamental à la vie privée et à la transparence et a noté que « *comme cette mesure s'applique à tous nos citoyens, le groupe Article 29 considère que l'opinion publique devrait être largement sollicitée pour montrer que le processus de prise de décision est fondé sur une évaluation complète et correcte* ».
56.. Jusqu'en décembre 2004, le Parlement était seulement consulté. Le Conseil a justifié la nécessité de l'adoption rapide du règlement pour satisfaire les demandes américaines et prévenir l'abandon du programme « *visa waiver* ». Mais il parait que les Etats-Unis ne vont pas prolonger le délai (voir la lettre du 31 mars 2005 du président du *US House Judiciary Committee* à la Commission et au Conseil, reproduit sur www.statewatch.org).
57.. Voir la communication de la Commission sur le développement de SIS II – COM (2003) 771 final.
58.. JO L 213, 15 juin 2004, p. 5.
59.. Avis 7/2004, doc. 11224/04, WP 96, 11 août 2004.
60.. COM (2004) 835 final, Bruxelles 28 décembre 2004.
61.. Comme Europol, Eurojust, l'Agence de la Gestion des Frontières, le *Police Chiefs Task Force*, et SitCen.
62.. Voir en particulier le programme de la Haye, paragraphes 2.1-2.5.
63.. Haggerty K.D. et Ericson R.V., « The Surveillant Assemblage », *British Journal of Sociology*, 51/4, 2000, p. 619. Voir aussi, notamment sur la transformation de la surveillance de réactive à proactive, Levi M., Wall D.S., « Technologies, Security and Privacy in the post-11 septembre European Information Society », *Journal of Law and Society*, 31/2, juin 2004, p. 194.
64.. « *It is increasingly difficult for individuals to maintain their anonymity or to escape the monitoring of social situations* ». David Lyon note que, malgré l'accent mis sur les développements dans le secteur privé/commercial quand on analyse la surveillance moderne, le rôle de l'Etat reste central. L'Etat peut utiliser les données assemblées par la surveillance « privée ». Voir « Surveillance after September 11, 2001 » in Ball K. et

Webster F. (dir.), *The Intensification of Surveillance*, Pluto Press, Londres, Sterling VA, pp. 21-22.

65.. Didier Bigo parle de populations satellites (« *satellite populations* ») qui sont considérées comme exceptionnelles et donc exclues de leur destination souhaitée. Voir « Criminalisation of 'Migrants': the Side Effect of the Will to Control the Frontiers and the Sovereign Illusion » in Szyszczak E. *et al* (dir.), *Irregular Migration and Human Rights*, Brill, Leiden, 2004, p. 91.

RÉSUMÉS

Ces dernières années les demandes d'intensification de la surveillance et des contrôles du mouvement des personnes au niveau mondial se sont développées. Cet article examine cette intensification de la surveillance au sein de l'UE en analysant la législation obligeant les transporteurs à fournir les données personnelles des passagers aux services d'immigration, un accord entre l'UE et les Etats-Unis sur le transfert des « *passenger name records* » (PNR) aux autorités américaines, et les plans européens d'introduction de données biométriques aux passeports et visas et d'amélioration de l'interopérabilité des bases de données européennes (SIS et VIS notamment). Ces développements, justifiés par un discours de « guerre au terrorisme », élargissent le réseau de la surveillance et soulèvent un certain nombre de questions sur la légitimité, la démocratie, et la protection des droits fondamentaux dans l'UE. Ils apparaissent également en décalage avec le concept de l'UE comme espace sans frontières. Ce texte abordera ces questions en analysant les négociations, le contenu et les implications de telles initiatives.

Recent years witnessed calls for the intensification of surveillance and the monitoring of people globally. This article will examine this intensification of surveillance in the European Union, by analysing legislation requiring carriers to transmit to immigration authorities passenger data, an agreement between the Community and the US on the transfer of passenger name records (PNR) to US authorities, and EU plans to introduce biometrics in passports and visas and enhance the interoperability of EU databases (such as SIS and VIS). These developments, justified by a 'war on terror' discourse, widen the net of surveillance and raise a number of questions regarding legitimacy, democracy and the protection of fundamental rights in the EU. They also appear to be at odds with the concept of the EU as a borderless area. The article will address these issues by analysing the negotiations, content and implications of these initiatives.

INDEX

Mots-clés : anti-terrorisme, étrangers, exception, flux, mobilité, surveillance

AUTEUR

VALSAMIS MITSILEGAS

Valsamis MITSILEGAS est professeur de droit à la Queen Mary University de Londres.