Les technologies européennes de contrôle de l'immigration

Vers une gestion électronique des « personnes à risque »

Ayse Ceyhan

Dans Réseaux 2010/1 n° 159 , pages 131 à 150
Éditions La Découverte

ISSN 0751-7971
ISBN 9782707159441
DOI 10.3917/res.159.0131
Date de mise en ligne : 01/02/2010

LES TECHNOLOGIES EUROPÉENNES DE CONTRÔLE DE L'IMMIGRATION

Vers une gestion électronique des « personnes à risque »

Ayse CEYHAN

DOI: 10.3917/res.159.0131

Dans le contexte de la « fluidité » qui caractérise notre temps (Bauman, 2000), les paramètres de la mobilité changent constamment. Ils ne suivent plus seulement les évolutions des moyens de production et du capital, mais sont de plus en plus déterminés par des motifs subjectifs, relationnels et familiaux qui modifient profondément les causes, la durée et la trajectoire des migrations (Diminescu, 2001). Dorénavant, ces migrations n'aspirent plus exclusivement à la sédentarisation dans le pays d'accueil, mais diversifient leur mode d'établissement en fonction des types de mobilité : sédentarisation, circulation, transit, retour au pays, ré-immigration, etc. (Withol de Wenden, 2008).

Toutefois, l'Union européenne hésite à faire de la mobilité un atout (*ibid.*). Plutôt que de bâtir une politique d'immigration adaptée aux nouvelles dynamiques de la mobilité, elle continue de mélanger une logique sécuritaire de contrôle, qu'elle valorise plus que tout, avec une logique utilitariste d'accueil de migrants qualifiés pour combler le manque de main-d'œuvre dans certains domaines bien précis comme l'informatique. Comme on a pu le voir dans le programme de la Haye adopté en 2004[1], les questions d'immigration sont incessamment liées avec celles du contrôle aux frontières, de la lutte contre le crime organisé, le terrorisme et la sécurisation des moyens d'identité. Lier ensemble des questions aussi diverses et antithétiques que celles-ci est une des caractéristiques les plus saillantes des discours sur la sécurité qui ont été énoncés depuis les années 1980, tant au niveau national qu'européen (Bigo, 1996, 1998). Toutefois, leur application au niveau européen s'est très vite heurtée à de grosses difficultés de gestion, de financement, de coordination et d'efficacité.

---

1. Adopté lors du Conseil européen de novembre 2004, ce programme a fixé dix priorités pour réaliser les objectifs de la politique européenne pour la période 2005-2010. Parmi ces priorités, celles qui portent sur le contrôle de l'immigration sont associées à la lutte contre l'immigration clandestine, la gestion des frontières extérieures, la lutte contre le terrorisme, la lutte contre le crime organisé, l'intégration des identifiants biométriques dans les documents de voyage et d'identité, etc. Voir *The Hague Programme: Strengthening Freedom, Security and Justice in the EU*, OJC 53, 33, 2005.

La conséquence la plus immédiate de l'interconnexion de ces domaines a été la quasi-impossibilité de gérer ce nouveau complexe avec des outils et des méthodes traditionnelles de gestion des flux. Il s'est avéré que la démarche méthodologique de classement, de catégorisation et de suivi n'était plus adaptable. Les statistiques des entrées et sorties, les fichiers des étrangers établis au niveau des États membres, les cartes de séjour, les visas attribués par les États, les fichiers de personnes recherchées, etc., ne suffisaient plus pour gérer un si grand nombre de problématiques auxquelles les migrants étaient associés. En effet, pour les autorités de contrôle, il ne s'agissait plus de se fier aux apparences, mais de détecter les véritables motifs de mobilité. Comment pouvait-on savoir si un simple touriste, un étudiant, une épouse d'immigré légal, un migrant, un jeune, etc., ne cachait pas en fait un illégal, un terroriste (actuel ou potentiel), un criminel ou un délinquant ? Comment pouvait-on déterminer le véritable motif de voyage des individus dans un contexte de mobilité de plus en plus intense, facilité par l'abolition des frontières internes de l'espace Schengen ? Comment allait-on être sûr qu'un demandeur d'asile n'était pas un « fraudeur », autrement dit, qui n'avait pas déjà déposé une demande d'asile dans un autre pays de l'UE ?

La solution à ces problèmes a été recherchée dans un recours aux technologies nouvelles d'identification et de surveillance, dont la caractéristique la plus saillante est d'être à la fois mobiles et intelligentes, c'est-à-dire capables de s'adapter à la mobilité des individus, de les suivre, de tracer leur itinéraire et de déterminer leur véritable identité (Ceyhan, 2006, 2008). Elles ont permis la mise sur pied progressive d'un dispositif intégrant des puces dans les visas et les documents de séjour, des lecteurs de puces, des caméras et des identifiants biométriques reliés à des bases de données conçues pour traiter les informations stockées en amont et recueillies pendant le voyage (SIS I et II, VIS, Eurodac).

Le caractère le plus saillant de ce dispositif est sa fonction proactive et prédictive. En effet, il n'est pas seulement destiné à gérer les flux migratoires, mais à détecter les « individus à risque » avant même leur entrée sur le sol européen. Pour le saisir dans toute sa complexité, il convient de l'analyser dans le cadre des « frontières intelligentes » où il constitue le fondement technologique d'un système de détection et de filtrage opérant sur plusieurs sites physiques et virtuels situés non seulement à la frontière physique, mais surtout à distance (en amont) dans le pays d'émigration. Cet article examinera les spécificités de ce dispositif en analysant le type de rationalité qu'il instaure avec les frontières intelligentes. Il explorera également l'impact que ce dispositif peut avoir sur les processus de subjectivation en se référant au concept foucaldien de gouvernementalité, entendu « au sens large de techni-

ques et procédures destinées à diriger la conduite des hommes » (Foucault, 1994, p. 124). Il étudiera la manière dont ce dispositif s'étend à la façon dont les migrants et les autres acteurs impliqués dans le processus de migration, comme les passeurs, se comportent, s'adaptent ou essaient de contourner les mesures adoptées. Plus généralement, il regardera si ce dispositif peut servir de grille d'analyse pour le régime de contrôle et de surveillance de la mobilité qui se met en place en Europe depuis l'adoption de la Convention des accords de Schengen en 1990 ; laquelle a créé la première grande base de données au niveau européen : le SIS (Schengen Information System)[2].

FAIRE DES FRONTIÈRES INTELLIGENTES UN SITE DE DÉTECTION DES PERSONNES À RISQUE

La mise sur pied des « frontières intelligentes » a entraîné une transformation de la manière de construire et de vivre la frontière. Désormais, la frontière s'adapte à la mobilité en devenant mobile elle-même et se transforme en un site d'analyse de risque effectuée à partir de la comparaison entre les informations fournies par le voyageur/migrant ressortissant d'un pays tiers et des informations contenues dans les puces électroniques des documents de voyage, ainsi que dans des bases de données européennes comme le SIS, le VIS et l'EURODAC.

Parallèlement à son sens physique comme distinguant l'intérieur de l'extérieur (Foucher, 1991), la frontière est investie de plusieurs significations qui font d'elle une référence hautement symbolique, non seulement pour les membres de la communauté nationale, mais aussi pour ceux qui veulent la franchir. Pour les premiers, elle est un mythomoteur d'identité et un terme discursif qui crée une communauté imaginée (Anderson, 1997). Mais, pour ceux qui doivent la franchir afin d'entrer dans le territoire d'un État membre de l'Union européenne qui l'autorisera ensuite à circuler dans l'espace Schengen, elle

2. La Convention d'application des accords Schengen (CAAS) signée le 19 juin 1990 et entrée en vigueur le 25 mars 1995, créant « l'espace Schengen », qui peut être défini comme le champ d'application territoriale des accords de Schengen signés en 1985 entre cinq États (France, Allemagne, Belgique, Luxembourg, Pays-Bas) pour instituer la libre circulation des personnes entre les pays signataires. La convention d'application avait pour tâche de déterminer les « mesures compensatoires » nécessaires à la suppression des frontières internes. La CAAS créera surtout la première grande base de données européenne : le Système d'information Schengen (SIS), clef de voûte de ces accords, destiné à mettre en place la première coopération policière et judiciaire pénale entre ses États membres.

est le lieu de la rencontre avec la police des frontières investie du pouvoir d'inclusion et d'exclusion (Salter, 2006, p. 172). C'est en effet cette police qui contrôle et (re)confirme le statut de l'individu et lui tend son passeport ou sa carte d'identité en lui donnant un statut national, européen, touriste, migrant, réfugié, demandeur d'asile, étudiant, voyageur en transit (*ibid*. p. 171).

De nos jours, le passage de la frontière ne se limite pas seulement à la confirmation de ce statut, mais également à l'identification des personnes « à risque » dont l'entrée et la circulation à l'intérieur du territoire national et par extension dans l'espace Schengen doit être empêchée. Rappelons que la détection des personnes « à risque » est une vieille préoccupation. Elle existe depuis que les frontières ont été investies, dès les traités de Westphalie en 1648, de la fonction de représentation de la souveraineté et de démarcation de l'interne de l'externe. Chaque État établit sa liste de personnes à risque en fonction des figures de l'ennemi et du danger qu'il construit à des moments historiques différents. Par exemple, si de nos jours quand on dit « personne à risque », on pense immédiatement au terroriste islamiste de type Al Qaeda, on pensait dans les années 1920 au commerçant qui vendait de l'alcool des deux côtés de la frontière entre le Mexique et les États-Unis ou, pendant la Guerre froide, à l'agent secret soviétique qui rentrait dans le territoire d'un État européen sous une fausse identité. Mais avec les frontières intelligentes, l'idée est d'évaluer et de déterminer le degré de dangerosité d'une personne avant même sa rencontre avec la police des frontières. Cette évaluation se fait au préalable, dans le pays de départ, au sein des consulats si le voyageur sollicite un visa, et dans les aéroports, lors de l'enregistrement avant l'embarquement à destination d'un pays européen (Bigo et Guild, 2003) ou américain (Adey, 2004 ; Salter, 2007).

La détection d'une « personne à risque » s'effectue à travers un système proactif dont l'objet est double : identifier les motifs du voyage des individus avant même de leur assigner un statut de « voyageur sans risque », établissant une sécurité pour l'Europe. Il s'agit également d'être certain que le voyageur ne va pas devenir un « illégal » c'est-à-dire rester sur le sol de l'UE au-delà de la date limite de son visa. Pour ce faire, l'Europe avait déjà mis en place une politique commune active en matière de visas en adoptant en 1995 « le visa Schengen » et créé la première grande base de données européenne : le Système d'information Schengen (SIS). Destiné à mettre en place la première coopération policière et judiciaire pénale entre ses États membres, le SIS avait établi un signalement spécifique aux étrangers : le « signalement aux fins de non-admission » ciblant spécifiquement les illégaux, les étrangers criminels et les étrangers sous surveillance. L'Europe avait déjà créé ainsi une immense

catégorie d'« indésirables » (Preuss-Laussinotte, 2000). Elle avait également jeté les bases de ses frontières électroniques (Diminescu, 2001 ; Broeders, 2007) qui, par ailleurs, ne recouvrent pas exactement les frontières de l'Union européenne, puisque quatre pays font partie de cet espace sans être membres de l'Union : l'Islande, la Norvège, la Suisse, le Liechtenstein. En revanche, deux pays membres de l'UE, le Royaume-Uni et l'Irlande, ont refusé d'y participer à l'origine, assouplissant toutefois ensuite leur position puisqu'ils participent désormais à certains de ses aspects (Preuss-Laussinotte, 2006).

Afin de rendre plus efficace la détection de l'étranger indésirable, l'Europe a créé le VIS (Visa Information System) qui a pour objectif l'identification des étrangers demandeurs de visa. Mais le véritable motif est celui de la fraude et de la simplification des procédures de demandes de visa, afin de prévenir le « visa shopping » et faciliter davantage les contrôles aux frontières. Cependant, le champ d'application du VIS est bien plus vaste, signant la mise en place d'un objectif plus général : celui de créer à terme une seule grande base de données, et, dans tous les cas, de permettre les connexions et les échanges de données entre les bases actuelles (Preuss-Laussinotte, 2009). Ainsi, il est précisé que le VIS doit également aider à l'identification de tout étranger en situation irrégulière, voire à la détermination du premier pays d'accueil dans le cadre d'éventuelles demandes d'asile, rejoignant ainsi tous les objectifs d'Eurodac, les liens entre ces deux bases étant précisés dans le règlement du 9 juillet 2008 [3]. Par la mise en place de ce dispositif électronique de détection en amont de toute tentative de fraude, l'Europe établit un régime de « triage » de migrants en fonction de leurs intentions (Lyon, 2003 ; Salter, 2006), et ce avant même leur entrée sur le sol du pays.

Le VIS prévoit également d'intégrer les technologies biométriques d'identification telles que les empreintes digitales dans les dispositifs de visa [4]. Le « visa biométrique » consiste à recueillir au préalable les empreintes digitales des dix doigts du demandeur et la prise de sa photo. Les données collectées alimenteront une banque de données consultable aux frontières de l'espace Schengen. Signalons toutefois que de nos jours l'équipement en technologie biométrique des consulats des pays européens dans les pays tiers n'est pas

3. Règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS).

4. L'introduction de la biométrie dans les visas fait suite à la décision n° 2004/512/EC du Conseil européen du 8 juin 2004. Il est prévu de la systématiser jusqu'en 2011.

définitivement achevé. Si dans certains pays africains comme le Mali ou la Côte d'Ivoire les consulats, dont celui de France, ont été parmi les premiers à l'expérimenter, tous les consulats des pays européens ne délivrent pas encore le visa biométrique.

L'Europe envisage également la création d'un système d'entrées et de sorties (Entry/Exit) comprenant les données de tous les ressortissants de pays tiers entrés par de multiples canaux (légalement, illégalement, en transit, etc.) (Frattini, 2008). L'objectif est alors de munir les services de police d'une base de données contenant les empreintes digitales de tous les étrangers, ainsi que leur date d'entrée, leur type de visa, etc. Toutefois, pour l'heure, les procédures de mise en œuvre de ce dispositif ne sont pas connues. Toujours est-il qu'en matière de corpus de dispositifs, on retrouve les mêmes mesures que l'administration américaine a déployées dans son plan « smart borders » adopté bien avant les attentats du 11 septembre dans le but de faire face à l'immigration clandestine, au trafic de drogue et au crime organisé (Ceyhan, 2004).

Les frontières intelligentes ont pour objectif d'adapter la sécurité à la fluidité. Il s'agit d'équiper les frontières terrestres et aériennes d'un réseau de surveillance technologique (senseurs, capteurs, biométrie, caméras de surveillance, etc.), à la fois pour détecter les personnes à risque et accélérer le passage des personnes qui ne posent pas de risque de sécurité. Depuis les attentats du 11 septembre, le Homeland Security Department (HSD) a mis sur pied l'US-VISIT, un ensemble de mesures de sécurité qui commence à l'étranger dans les bureaux de délivrance de visas dans les consulats américains et se poursuit jusqu'aux procédures de contrôle dans l'aéroport de départ et à l'arrivée aux États-Unis (la collecte des empreintes digitales). Ce système couplé avec la loi sur la sécurité aux frontières et le visa (Enhanced Border Security and Visa Entry Reform Act du 9 mai 2002) qui impose aux compagnies aériennes assurant la liaison à destination, au départ et à travers les États-Unis de transmettre aux services des douanes et de l'immigration américains des informations personnelles sur les passagers, repose sur un système électronique de *data mining* et de statistique décisionnelle permettant de dégager des profils de dangerosité à partir desquels les personnes sont déclarées « à risque » ou « sans risque » (Lyon, 2003 ; Salter, 2007 ; Ceyhan, 2008).

Dans ce dispositif, l'élément qui a le plus attiré l'attention des autorités européennes est le PNR (Personal Name Record) – les données de dossiers passagers – auquel recourt l'Administration américaine pour renforcer la sécurité d'aviation. Il s'agit d'une base de données qui contient les données personnelles sur les détails de voyage des passagers. Elle est créée soit par le biais

d'un système de réservation informatique (GDS), soit directement par une compagnie aérienne ou ferroviaire. Les données personnelles portent sur le nom, l'itinéraire, les moyens de paiement du billet, les réservations d'hôtel et de voiture et les préférences (siège, plateau-repas, etc.). Il convient de rappeler que le stockage de ce type de données est une pratique ancienne effectuée depuis longtemps par les compagnies d'aviation, pour des raisons de marketing et d'échange au sein du secteur du tourisme. Les données sont exploitées par quatre compagnies privées : Sabre, Amadeus, Galileo, Worldspan. Depuis le 11 septembre, cette pratique est devenue un moyen pour échanger les données personnelles des passagers entre l'Union européenne et les États-Unis dans un but officiel de lutte contre le terrorisme et l'immigration clandestine. Les données contenues dans ces bases de données sont traitées afin de savoir à l'avance si un passager est un terroriste connu ou un terroriste potentiel. Cependant, en raison de son traitement des données à caractère personnel, ce système a été fortement critiqué par le Parlement européen, le Contrôleur européen des données personnelles (CEDP) et le G-29[5], pour manque de dispositions sérieuses protégeant les données personnelles et la vie privée des passagers, surtout aux États-Unis où la législation ne contient pas de mesures de protection semblables à celles adoptées par la directive européenne de 1995[6]. Toutefois, ces critiques n'ont pas empêché l'Union européenne de signer l'accord PNR du 7 juillet 2007 avec Washington et de décider d'adopter un système similaire pour stocker pendant treize ans les données personnelles des voyageurs des pays tiers à destination de l'un des pays de l'UE.

Conjointement à ce régime de « détection de personnes à risque et de triage d'intentions », l'Europe poursuit sa construction des frontières intelligentes en mettant sur pied un modèle intégré de gestion des frontières[7]. Pour ce faire,

---

5. G-29. Avis commun à la proposition de décision cadre du Conseil relative à l'utilisation des PNR à des fins répressives, le 6 novembre 2007, 02/22/07/EU.

6. Pour de plus amples détails sur ces critiques, voir Preuss-Laussinotte (2006).

7. La gestion des frontières comporte essentiellement cinq dimensions : 1) contrôle des frontières : vérification et surveillance, analyse de risques et opérations de renseignement en matière pénale ; 2) détection de la criminalité transfrontalière et enquêtes ; 3) adoption du modèle de contrôle de l'accès à quatre niveaux (mesures dans les pays tiers, coopération avec les pays voisins, contrôles aux frontières et mesures de contrôle dans le domaine de libre circulation ; 4) coopération entre services chargés de la gestion des frontières (gardes frontières, services douaniers, police, services de sécurité nationale et autres autorités compétentes et coopération internationale ; 5) coordination et cohérence des activités des États membres et des institutions et autres organes de la Communauté, Conseil de l'UE, Communiqué de presse 2786e session, Justice et Affaires intérieures, 15801/06, Bruxelles, 4-5 décembre 2006.

elle a créé en 2005 l'agence FRONTEX[8]. Au-delà des mesures opérationnelles, FRONTEX doit effectuer des analyses de risque en mettant au point un modèle d'évaluation commune et intégrée des risques généraux et spécifiques, suivre l'évolution de la recherche dans les domaines présentant un intérêt avec la surveillance des frontières. Ainsi en 2007, son directeur a déclaré : « La migration illégale à destination de l'Union européenne emprunte quatre itinéraires principaux ; il s'agit là du passage par les frontières maritimes extérieures du Sud, par les frontières terrestres extérieures de l'Est, par les Balkans, ainsi que par les aéroports internationaux[9]. » Parallèlement, la Commission a présenté une communication (COM (2008) 68 final) proposant une feuille de route pour l'établissement et la mise en place d'un système européen de surveillance des frontières (EUROSUR). Celui-ci couvrira les frontières terrestres et maritimes de l'UE et sa mission principale sera de fournir aux États membres des informations stratégiques pour la surveillance de ces frontières et de faciliter l'application commune des dispositifs de surveillance par les États membres en temps réel, grâce à un réseau de communication renforcé par les technologies sophistiquées de communication et d'information.

On voit que l'Europe veut ainsi mettre sur pied un système intégré reliant les frontières terrestres et maritimes à travers des dispositifs communs de surveillance et de communication. Or la mise en œuvre de ce système est très coûteuse[10] et nécessite une coopération étroite entre les différents États membres ainsi qu'entre les agences de sécurité, ce qui est loin d'être acquis à l'heure actuelle[11].

Au terme de ce survol des différentes étapes de la construction d'un dispositif dont le principal point focal est la détection en amont de « personnes à risque », on peut se demander si l'Europe a élaboré une définition claire et nette de cette notion. Notant son absence au niveau européen, nombreux observateurs ont souligné l'absence même d'une catégorie juridique claire de la

---

8. Règlement CE n° 2007/2004 du Conseil du 26 octobre 2004, JO L 349 du 25 novembre 2004.

9. Déclaration d'Ilka Laitinen, directeur du FRONTEX, EU 2007, Présidence de la République fédérale d'Allemagne, EU 2007 DE, Communiqué de presse, 22 février 2007.

10. Le budget de Frontex est passé de 6 millions d'euros en 2005 à 80 millions d'euros en 2009, voir *European Voice's eNews*, 1er octobre 2009.

11. Citons par exemple les critiques des autorités françaises à l'encontre du FRONTEX après l'échec d'une opération commune à l'encontre des sans-papiers de Malte pendant l'été 2009. La France s'est plainte du manque de feuille de route claire et de répartition de compétences entre les États qui participent à ce type d'opérations. Voir *European Voice's eNews*, 1er octobre 2009.

notion d'immigré illégal en montrant l'imbrication des définitions existantes avec les enjeux nationaux définis en fonction de la perception politique des dangers dans le champ politique (Balzacq *et al*., 2006).

L'OBSESSION DE LA FRAUDE : LE RECOURS À LA BIOMÉTRIE

Le second point focal des frontières intelligentes est la fraude à l'identité et aux documents. Assigner une identité reconnaissable à quelqu'un et savoir avec certitude qui est qui, est devenu une préoccupation majeure depuis la fin de la Guerre froide avec la disparition de l'ennemi communiste et les développements de la globalisation (Ceyhan, 2006b). Aux yeux des agences de sécurité et des polices de l'immigration, les moyens traditionnels d'identification comme la carte nationale d'identité et le passeport ainsi que les identifiants classiques comme le nom patronymique, l'âge, le sexe, la filiation, et même le visa, seraient devenus de moins en moins pertinents pour prouver l'identité d'une personne. Les spécialistes justifient le lien entre identité et sécurité par l'augmentation de la fraude à l'identité (création d'identité fictive, usurpation d'identité, échange d'identité, utilisation de l'identité d'une personne décédée, etc.), qui aurait pris, ces dernières années, des proportions considérables. Dans tous les pays européens et aux États-Unis, les techniques de fraude comme le vol de titres vierges, la falsification des données, la contrefaçon, l'usage frauduleux d'un titre authentique volé ou emprunté à une personne, les vrais faux documents seraient en constante augmentation.

Afin de pouvoir identifier les migrants et les demandeurs d'asile (tout comme les nationaux d'ailleurs) avec certitude, le recours aux technologies de pointe comme la biométrie est présenté comme le moyen le plus sûr d'authentification et d'identification (Ceyhan, 2006b, 2008). La biométrie consiste à transformer les caractéristiques biologiques, morphologiques et comportementales d'une personne comme les empreintes digitales, l'empreinte de la rétine de l'iris, la voix, la forme du visage et de la main, etc., en une empreinte numérique. Fondée sur l'hypothèse que la probabilité que deux personnes possèdent les mêmes caractéristiques biologiques, génétiques ou morphologiques est infime, la biométrie est considérée comme la solution scientifique qui établit et atteste de l'unicité d'une personne. Celle-ci est garantie avec l'établissement d'un lien unique entre les caractéristiques biométriques et son porteur.

L'Europe a choisi de confronter les identifiants fournis par les demandeurs de visa et les demandeurs d'asile avec les informations qu'elle a conservées

dans les bases de données lesquelles ont également commencé à intégrer les éléments biométriques pour plus de certitude.

La première grande base de données biométriques est l'Eurodac (Van der Ploeg, 1999a). Elle a été créée dans le cadre de la politique d'asile européenne. Son objectif est de savoir si le demandeur d'asile n'est pas un « fraudeur » – autrement dit, s'il n'a pas déjà déposé une demande d'asile dans un autre pays de l'UE –, afin d'éviter ce qu'on désigne sous l'expression « *asylum shopping* ». Plus globalement, il vise à enregistrer les empreintes digitales de tous les étrangers appréhendés à l'occasion d'un franchissement irrégulier d'« une frontière extérieure » à l'Union européenne (Chapitre 3 du règlement Eurodac), et de ceux qui se trouvent illégalement sur le territoire d'un État membre de l'UE (Chapitre 4). La base de données Eurodac fonctionne avec un système d'échanges et de comparaison : chaque État enregistre les empreintes digitales de ses demandeurs d'asile (et autres) âgés de plus de 14 ans, et les transmet à l'unité centrale, à la fois pour que ces empreintes y soient enregistrées, et pour qu'une comparaison soit effectuée avec les empreintes qui y figurent déjà. Il faudra également préciser qu'Eurodac fonctionne sur le modèle du SIS, avec une unité centrale gérée par la Commission européenne, et des unités nationales qui lui sont reliées. Les données dactyloscopiques transmises par un État membre sont comparées par l'unité centrale avec celles qui ont été transmises par d'autres États membres et déjà enregistrées. L'unité centrale transmet sans délai le résultat positif, ou négatif, de la comparaison à l'État membre d'origine, selon le système « hit/no hit » (concordance/non-concordance) (Preuss-Laussinotte, 2009).

Conçu à l'origine pour les demandeurs d'asile et étendu par la suite à toute l'immigration illégale, l'Eurodac entre en concurrence avec une autre base de données, le SIS II, la version réactualisée du SIS. En effet, le SIS, devenu inadapté aux évolutions techniques a été remplacé par le SIS II, dont l'objectif est plus large que le contrôle des flux migratoires, mais qui reste un instrument essentiel pour ce contrôle, d'autant qu'il intègre lui aussi des données biométriques, c'est-à-dire les empreintes digitales des étrangers « aux fins de non-admission ».

Dans le même temps, le fonctionnement du SIS devrait être complété par la mise en œuvre d'échanges de données biométriques entre les États de l'Union européenne, notamment des données génétiques, décidé dans le cadre du Traité de Prüm. Signé le 25 mai 2005 entre l'Autriche, la France, la Belgique, l'Allemagne, l'Espagne, le Luxembourg et les Pays-Bas, l'accord de Prüm

est intégré dans le cadre de l'Union européenne par décision de 2008. Le traitement et l'échange de données à caractère personnel sont au cœur du Traité de Prüm. Ce traité qui vise à accélérer la coopération européenne en matière de consultation automatique et d'échange de données en se basant sur le « principe de disponibilité » [12] prévoit l'échange de données génétiques, d'empreintes digitales, de données de plaques d'immatriculation afin de prévenir des attaques terroristes et de lutter contre l'immigration clandestine. Ce type d'échange nécessite cependant une interopérabilité des systèmes impliquant l'adoption de normes techniques communes entre différents pays et au sein même des pays entre différentes agences, qui est encore loin d'être aboutie (Preuss-Laussinotte, 2009 ; Balzacq *et al*., 2006).

L'ensemble est complexe, et aboutit à la création de plusieurs grandes bases de données biométriques dont la priorité est d'abord le contrôle des étrangers, mais dont la compétence s'étend progressivement à d'autres objectifs : lutte contre le terrorisme, lutte contre la délinquance, et plus généralement, protection de la sécurité intérieure et extérieure de l'UE et de ses États membres (Preuss-Laussinotte, 2006).

Comment caractériser cet ensemble ? S'agit-il d'un Léviathan, d'un Big Brother, d'un panoptique à l'échelle européenne ? Pour l'appréhender, la métaphore du « rhizome » paraît plus adéquate que ces références précitées. La détection des « personnes à risques » s'opère dans un système discret constitué d'objets et de données hétérogènes et mouvantes, structuré à l'image d'un rhizome, métaphore développée par Deleuze et Guattari dans *Mille Plateaux* (1980, pp. 9-38). Selon ces deux auteurs, le rhizome pourrait être envisagé comme « une tige souterraine se distinguant absolument des racines et des radicelles ». « Il n'impose pas une structure hiérarchique et prend des formes très diverses, depuis son extension superficielle ramifiée en tous sens jusqu'à ses concrétions en bulbes et tubercules » (*ibid*., p. 13). Son unité tient seulement au fonctionnement des objets multiples et hétérogènes comme un ensemble. On peut dire suivant les analyses que font Kevin Haggerty et Richard Ericsson (2000) de la surveillance après le 11 septembre, que la détection du migrant indésirable procède de l'image du rhizome non hiérar-

12. « Principle of availability ». Selon ce principe, les autorités d'un État membre ont le même droit d'accès à l'information détenue par une autre autorité dans l'Union, comme il est également appliqué aux autorités étatiques au sein de l'État où les données sont stockées ; voir Proposal for a Community Framework Decision as the Exchange of Information Under the Principle of Availability, COM (2005) 490 Final, Bruxelles, 12 octobre 2005.

chique, qui opère en deux temps. Il s'agit d'abord de l'extraction du corps de l'individu de sa place fixe (par les techniques biométriques et les bases de données). Suit l'introduction de ce corps dans un flux de données en circulation qui seront réassemblées dans des lieux et sites différents, sous forme de catégories créées pour distinguer les individus en fonction de leur profil et de leur degré de dangerosité. Dans ce système, ce sont les parties inchangeables du corps de l'individu et ses données personnelles qui circulent à travers les ramifications et sont ensuite recomposées dans des configurations informatiques pour être comparées aux profils préétablis. Ce sont donc les profils qui remplacent l'identité d'une personne qui n'est reconnue que par l'empreinte informatisée de ses éléments biométriques et de critères comme la propension à voyager (voyageur fréquent), le goût (les préférences alimentaires), l'appartenance à des réseaux (ethnique, professionnel, religieux), etc. Cependant, cette façon d'identifier les personnes est profondément problématique car elle réduit l'identité, processus complexe, à de simples catégories facilement reconnaissables et classables dans des banques de données. L'identité devient alors la réduction des propriétés biométriques de l'individu à des données informatiques extraites des empreintes de son corps et une correspondance à un ensemble de profils préétablis (Van der Ploeg, 2002 ; Ceyhan, 2006a). Cette transformation de l'identité en données informatiques génère des interrogations profondes quant à la protection des données personnelles à partir de l'assemblage desquelles les autorités nationales et européennes bâtissent les figures de la dangerosité.

UNE GOUVERNEMENTALITÉ PAR LA TECHNOLOGIE : INTÉRIORISATION, CONFESSION, PROFESSIONNALISATION

Cet ensemble qui ressemble davantage à un assemblage de différentes technologies qu'à un système homogène peut être également appréhendé à partir du concept foucaldien de dispositif défini comme « un ensemble résolument hétérogène comportant des discours, des institutions, des aménagements architecturaux, des décisions réglementaires, des lois, des mesures administratives, des énoncés scientifiques, des propositions philosophiques, morales, philanthropiques ; bref, du dit aussi bien que du non-dit, voilà les éléments du dispositif. Le dispositif lui-même, c'est le réseau qu'on établit entre ces éléments […] par dispositif, j'entends une sorte – disons – de formation qui, à un moment donné, a eu pour fonction majeure de répondre à une urgence » (Foucault, 1994, p. 299). L'ensemble inclut les discours, les techniques, les technologies, les mesures, les projets, les plans, les modèles, et s'inscrit toujours dans une relation de pouvoir.

Dans cette section, nous nous intéresserons à l'impact de ce dispositif sur les migrants à partir de la notion de gouvernementalité. Dans son analyse des « arts de gouverner », Foucault a montré que le pouvoir ne se réduisait pas au seul contrôle du territoire et de l'institution, mais s'étendait au gouvernement des hommes, des individus ou des collectivités (Foucault, 2004, p. 126). Il a appelé « gouvernementalité » le régime de pouvoir mis en place au dix-huitième siècle qui « a pour cible principale la population, pour forme majeure de savoir l'économie politique, pour instrument technique essentiel les dispositifs de sécurité » (*ibid*.). Portant au départ sur les techniques de gouvernement qui sous-tendent la formation de l'État moderne, la gouvernementalité a ensuite été entendue « au sens large de techniques et procédures destinées à diriger la conduite des hommes. Gouvernement des enfants, gouvernement des âmes ou des consciences, gouvernement d'une maison, d'un État ou de soi-même » (Foucault, 1994, p. 124).

Le principal axe par lequel la gouvernementalité joue sur les comportements des individus qui sont en mouvement, que ce soient des touristes ou des migrants, est la détection de « personnes à risque ». À la lumière des travaux d'Ulrich Beck (1986), on peut se demander si la détection du risque dont les autorités de l'immigration parlent se situe à la fois sur le présent et surtout sur l'avenir. La réponse semble positive. La détection s'inscrit en effet dans le passé, l'individu pouvant être fiché dans une base de données comme un sans-papier, un expulsé, un *asylum shopper*, un criminel, etc. Mais elle se place aussi dans le futur, puisqu'il peut rentrer sur le territoire de l'espace Schengen avec un visa en règle, mais ne pas respecter sa date d'expiration et s'établir dans un pays européen. Dans la société du risque, c'est l'anticipation du futur risque – donc pas totalement précis – qui prend une fonction déterminante. Pour ce qui est de l'immigration, les bases de données devenant de plus en plus intelligentes, c'est-à-dire portant sur le traitement et le croisement de l'information et établissant des profils de dangerosité, il s'agit essentiellement de déterminer les risques à venir.

Cette détection de risque à double temporalité s'effectue en amont lors du dépôt des documents pour obtenir un visa, dans le pays d'immigration lors du renouvellement de la carte de séjour et à la frontière aérienne, terrestre (et dorénavant maritime), non seulement des pays de l'espace Schengen, mais de tous ceux où le migrant doit entrer avec un visa. Selon Mark Salter qui a étudié le régime global de visas et les technologies de contrôle de voyageurs et/ou migrants dans les aéroports, la gouvernementalité s'exerce par « un ensemble confessionnel » composé d'« obéissance inconditionnelle (à l'agent de

police), d'un examen non interrompu et d'une « confession exhaustive » de la part de l'individu (à l'agent consulaire et/ou à l'agent de police) (Salter, 2006, pp. 180-181). Face à l'agent consulaire ou celui de la compagnie aérienne qui interroge avant l'embarquement, ou la police des frontières qui contrôle les documents, l'individu se présente en ayant préalablement intériorisé le fait qu'il va être examiné ou interrogé en fonction du profil de la « personne à risque » qu'il peut représenter et s'engage alors dans un processus confessionnel afin de prouver qu'il ne constitue pas de risque pour le pays en question. La confession porte sur les motifs du voyage et/ou du séjour, les itinéraires, les relations, l'occupation et comporte même une promesse de retour au pays sans dépasser la date de validité du visa.

Cependant, la confession ne doit pas dépasser le cadre des questions préétablies, c'est-à-dire ne doit pas porter sur des sujets qui ne sont pas dans la *check list* des officiers, sinon elle peut générer de la suspicion. En d'autres termes, il faudra répondre avec des réponses standard aux questions posées, mais ne pas raconter sa vie, sinon cela devient suspect. Pendant que le migrant et/ou le voyageur ressortissant d'un pays tiers s'attelle « à confesser », les documents présentés à l'officier de la police confirment ou infirment la confession à travers la lecture électronique des données qu'ils contiennent et de leur comparaison avec des bases de données (SIS II, VIS, EURODAC).

Le corps fait aussi partie de l'ensemble confessionnel (Salter, 2006, p. 183). Il y participe non seulement à travers ses expressions, mouvements, tics, odeurs, etc., mais aussi à travers sa lecture par les caméras de chaleur, de détection de maladies, de mouvements anormaux qui, même si ces caméras ne sont pas déployées à grande échelle, font partie du dispositif de contrôle. Le corps sert ainsi de témoin en faveur ou contre le narratif énoncé par le migrant lors de son interaction avec la police des frontières et/ou les services de l'immigration. Il joue ainsi un rôle fondamental en servant de site d'identification (Van der Ploeg, 1999a ; Ceyhan, 2006a, 2008) et de détermination de la légalité ou de l'illégalité du migrant et du demandeur d'asile (Van der Ploeg, 1999b). Ainsi, dans son analyse de l'EURODAC, Irma van der Ploeg montre qu'avec l'introduction des empreintes biométriques dans les documents et leur informatisation, c'est le corps qui informe sur le statut du migrant et devient un site de détermination de la légalité ou de l'illégalité (Van der Ploeg, 1999a).

La combinaison de la confession et de la lecture du corps est en train de mettre sur pied une nouvelle forme de gouvernementalité dont les contours sont en gestation, mais dont on peut dès maintenant percevoir quelques signes

d'impact sur les migrants et les passeurs. Selon Dana Diminescu (2001), « les frontières informatiques ont déjà contribué à la modification des stratégies de départ et de la composition du capital de la mobilité » générant des pratiques de détournement et d'adaptation aux nouvelles technologies. La conséquence la plus immédiate est la « professionnalisation informatique des passeurs » qui déploient les mêmes types de connaissances que les fabricants de systèmes informatiques pour les contourner, et la mise en réseau des moyens de contournement (*ibid*.). La frontière devient ainsi le lieu d'apprentissage et d'appropriation des nouvelles technologies. Cette « course » à l'appropriation des nouvelles technologies fait partie du quotidien des migrants et des passeurs, comme on peut l'observer à la frontière américano-mexicaine qualifiée de « laboratoire interactif » de fabrication de nouveaux dispositifs intelligents de sécurité et de surveillance et des techniques de contournement (Andreas, 2003 ; Ceyhan, 2004, 2008). L'étude de Dana Diminescu montre combien ces techniques s'universalisent et s'adaptent en même temps à chaque cas. Les « professionnels du passage des frontières » importent ainsi les techniques d'ailleurs, tout en créant leurs propres arts du passage. Il ne faut cependant pas oublier de rappeler que cette technologisation des fonctions de contrôle et de surveillance, tout en entraînant la technologisation des stratégies de contournement, s'accompagne aussi du recours à des stratégies plus traditionnelles comme le mariage avec un(e) ressortissant(e) européen(ne), les entrées clandestines par des chemins non technologiquement contrôlés, le dépassement de la date limite des visas, etc. (Diminescu, 2001).

Les frontières intelligentes font aussi apparaître un réseau hétérogène d'acteurs de contrôle, chacun étant spécialisé dans le maniement d'une nouvelle technologie : biométrie pour les uns, surveillance intelligente pour les autres ; la collecte de l'information pour les uns, le traitement de l'information pour les autres. La plupart de ces acteurs ne connaissent même pas l'existence des autres, ce qui explique par ailleurs la difficulté de mettre en place une coopération accrue au sein de FRONTEX.

Plutôt que de concevoir la mobilité des ressortissants des pays tiers et des migrants comme un atout, l'Europe la considère comme suspecte. Elle tend à transformer la gestion de l'immigration en une détection des véritables motifs de la mobilité. Pour ce faire, elle recourt aux nouvelles technologies d'identification et de surveillance qui, couplées à des bases de données, constituent un dispositif intelligent pour détecter et filtrer les « personnes à risque ». L'appellation « personne à risque » est malléable et peut porter sur plusieurs catégories de personnes : les terroristes connus, c'est-à-dire déjà inscrits dans des

bases de données des services de renseignements et de police, les personnes interdites de séjour, les demandeurs d'asile dont la demande a été rejetée, les disparus, les personnes soumises à une surveillance discrète, les personnes porteuses de maladies contagieuses, etc. Son emploi dans des domaines aussi variés que ceux-ci témoigne de l'intégration de la question de l'immigration dans une problématique plus vaste qui est celle de la sécurité (laquelle comprend aussi bien la sécurité intérieure que la sécurité globale). Ce faisant, l'Europe, tout comme les États membres, transforme l'objet et les procédés mêmes de la politique de l'immigration. Au lieu d'être menée par des « mesures normales » des politiques publiques, l'immigration est traitée comme « une menace existentielle qui appelle des mesures d'urgence et un discours de justification situés au-delà des procédures politiques normales » (Waever, 1995). Ces mesures caractérisent le passage d'un système réactif classique à un système proactif de contrôle et d'anticipation dont l'objectif est d'identifier les risques probables. L'immigration fait ainsi partie des problématiques inscrites dans le paradigme de risque à travers lequel les sociétés modernes cherchent à maîtriser les incertitudes contemporaines.

RÉFÉRENCES

ADEY P. (2004), "Secured and Sorted Mobilities: Examples from the Airport", *Surveillance & Society*, 1(4) online.

ANDERSON M. (1997), *Frontiers. Territory and State Formation in the Modern World*, London, Polity Press.

ANDREAS, P (2003), *The Rebordering of North America. Integration and Exclusion in a New Security Context*, London, New York, Routledge.

BALZACQ T., BIGO D., CARRERA S., GUILD E. (2006), "Security and the Two-Level Game. The Treaty of Prüm, the EU and the Management of Threats", *CEPS Working Documents*, n° 234, janvier.

BAUMAN Z. (2000), *Liquid Modernity*, Cambridge, Polity Press.

BECK U. (1986), *La société du risque*, Paris, Aubier/Alto.

BIGO D. (1996), *Polices en réseaux. L'expérience européenne*, Paris, Presses de Sciences Po.

BIGO D. (1998), « Sécurité et immigration : vers une gouvernementalité par l'inquiétude », *Cultures & Conflits*, n° 31, pp. 13-38.

BIGO D. et GUILD E. (2003), « La logique du visa Schengen : police à distance », *Cultures & Conflits*, n° 49, pp. 5-137.

BROEDERS D. (2007), "The New Digital Borders of Europe: EU- Database and the Surveillance of Irregular Migrants", *International Sociology*, vol. 22, n° 1, pp. 71-92.

CEYHAN A. (2004), « Sécurité et frontières aux États-Unis après le 11 Septembre », *Cultures & Conflits*, pp. 113-147.

CEYHAN A (2006a), « Technologie et sécurité : une gouvernance libérale dans un contexte d'incertitudes », *Cultures et Conflits*, n° 64, pp. 11-33.

CEYHAN A., (2006b), « Enjeux d'identification et de surveillance à l'heure de la biométrie », *Cultures & Conflits*, n° 64, pp. 33-49.

CEYHAN A. (2008), "Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics", *Surveillance & Society*, No. 5(2) online.

DELEUZE G. et GUATTARI F. (1980), *Mille Plateaux*, Paris, Les Éditions de Minuit.

DIMINESCU D. (2001), « Les frontières informatiques. Le système D contre le SIS », *Hommes & Migrations*, n° 1230, mars avril, pp. 28-34.

HAGGERTY K.D. et ERICSON R.V. (2000), "The surveillant assemblage", *British Journal of Sociology*, vol. 51, n° 4, décembre, pp. 605-622

European Commission (2008), *Examining the Creation of a European Border Surveillance System (EUROSUR) – Impact assessment*. Commission Staff Working Document SEC (2008) 152, Brussels, 13 February.

Fondation Robert Schuman (2006), « L'Union européenne et l'immigration », *Questions d'Europe*, 23 octobre, n° 42.

FOUCAULT M. (2004), *Sécurité, territoire, population. Cours au Collège de France 1977-1978*, Paris, Gallimard/Seuil.

FOUCAULT M. (1994), *Dits et Écrits*, *1954-1988*, Vol. III, Paris, Gallimard.

FOUCHER M. (1988, 1991), *Fronts et Frontières. Un tour du monde de géopolitique,* Paris, Fayard.

FRATTINI F. (2008), "Providing Europe with the Tools to Bring it Into the 21st Century", 12 March, Speech 09/142.

LYON D. (2003), "Airports as Data Filters: Converging Surveillance Systems after September 11", *Information, Communication and Ethics in Society*, Frank Cass, 1-27.

PLOEG Van der I. (1999a), "Eurodac and the Illegal Body. The Politics of Biometric Identity", *Computers and Society*, 29, 1, pp. 37-44.

PLOEG Van der, I. (1999b), "Written on the Body: Biometrics and Identity", *Computers and Society*, n° 29, pp. 37-44.

PLOEG Van der, I. (2002), "Biometrics and the Body as an Information: Normative Issues in the Socio-technical Coding of the Body", in Lyon David (Ed.), *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, New York, Routledge, pp. 57-73.

PREUSS-LAUSSINOTTE S. (2000), *Les fichiers et les étrangers au cœur des nouvelles politiques de sécurité*, Paris, LGDJ.

PREUSS-LAUSSINOTTE S. (2006), « L'Union européenne et les technologies de sécurité », *Cultures & Conflits*, n° 64, pp. 97-109.

Preuss-Laussinotte S. (2009), « Fichiers informatiques », in *Dictionnaire permanent droit des étrangers*, Paris, Éditions Législatives.

Preuss-Laussinotte S. (à paraître), « L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité » *Culture & Conflits.*

SALTER M. B. (2006), "The Global Visa Regime and the political Technologies of the International Self: Borders, Bodies, Biopolitics", *Alternatives* 31, 167-189.

SALTER M. B. (2007), "Governmentalities of an Airport: Heterotopia and Confession", *International Political Sociology*, n° 1, pp. 49-66.

WAEVER O. (1995), "Securitization, Desecuritization", in Lipschutz R.D. (Ed.), *On Security*, New York, Columbia University Press.

WITHOL de Wenden C. (2008), « Démographie, Immigration, Intégration », *Questions d'Europe*, Fondation Robert Schuman, 13 octobre.