ESPACE, POPULATIONS, SOCIETES, 2012-3 pp. 49-62

Rocco BELLANOVA

PRIO
Hausmanns gate 7
NO-0186 OSLO
Norvège
rbellano@vub.ac.be

Denis DUEZ

Université Saint-Louis - Bruxelles
43, boulevard du jardin botanique
1000 Bruxelles
Belgique
duez@fusl.ac.be

Le citoyen face aux nouvelles pratiques sécuritaires de l'Union européenne : enjeux démocratiques d'une sécurité par les fichiers

INTRODUCTION

Le traité d'Amsterdam a fait de la réalisation d'un espace de liberté, de sécurité et de justice (ELSJ) l'un des objectifs majeurs de l'Union européenne (UE). L'adoption de cet objectif politique général s'est traduite par la mise en œuvre progressive d'une politique européenne de sécurité intérieure. Le fait de circuler librement et en toute sécurité au sein d'un espace sans frontières a été considéré comme l'un des principaux attributs de la citoyenneté européenne. Cependant, ce déblocage des mobilités individuelles n'a été accompli qu'au prix de la mise en place de dispositifs de contrôle visant à surveiller ces mobilités et à empêcher les déplacements jugés illégitimes ou indésirables. Cette relation dynamique entre la promotion de la mobilité individuelle, les pratiques de contrôle qui les accompagnent et les dispositifs d'encadrement juridique de ces contrôles apparaît révélatrice d'une manière de penser la sécurité intérieure dans l'espace européen, mais aussi au-delà.

Cet article examine cette implication croissante de l'UE dans le champ de la sécurité intérieure selon deux angles d'approche. Il s'agit tout d'abord d'examiner les mutations des modalités de l'action publique à l'œuvre dans le champ de la sécurité en les replaçant dans une perspective du temps long. Nous montrerons que l'irruption des acteurs européens dans ce domaine prolonge et amplifie

un processus socio-historique marqué par la redéfinition des modes de gouvernance sécuritaire. Nous verrons en particulier que, dans la mesure où les moyens de la coercition restent attachés aux États membres, la pratique de l'Union en matière de sécurité suppose le passage de la logique de la « police », qui repose au premier chef sur la monopolisation des moyens de la coercition physique légitime, à celle du « *policing* », qui suppose un recours généralisé aux techniques – plus douces – de contrôle social. La notion de « contrôle social » renvoie ici à « l'existence, inhérente à toute société, de mécanismes de régulation qui conduisent chacun de ses membres à intérioriser les prescriptions d'un système de normes et de valeurs unique et stable ». Elle désigne également « l'ensemble de ces dispositifs de surveillance et de répression mis en œuvre par des instances spécialisées (police, justice, armées, école, etc.) afin d'asseoir le pouvoir d'un groupe dominant, en reconduisant les conditions de l'asservissement des dominés » [Ogien, 2006]. De fait, les pratiques sécuritaires contemporaines reposent de plus en plus sur des techniques de surveillance rendues possibles par l'évolution des technologies de l'information et de la communication. Appréhender les mutations des pratiques sécuritaires implique par conséquent de prendre au sérieux la place et le rôle des technologies dans ce contexte nouveau.

Au départ de cette réflexion sur les nouvelles manières *de faire* la sécurité, il s'agit ensuite de questionner l'impact des mutations à l'œuvre sur la nature et la substance du lien démocratique. Développées au nom du citoyen européen et de sa sécurité, ces évolutions ne finissent-elles pas par se retourner contre lui en détériorant l'équilibre entre sécurité et liberté caractérisant la relation gouvernants-gouvernés dans les sociétés démocratiques ? Le développement des technologies et des pratiques de surveillance et leurs rôles dans le façonnement d'un nouveau modèle de société est devenu un sujet crucial tant au niveau académique que socio-politique. La « société de contrôle » de Gilles Deleuze [1990, pp. 240-247], la « société panoptique » de Michel Foucault [1975] ou encore le sempiternel *Big Brother* orwellien sont des références de plus en communes dans ces débats. Pour autant, nous montrerons qu'il faut sans doute moins craindre à l'heure actuelle les formes d'oppression décrites par George Orwell qu'une certaine banalisation et dépolitisation de la surveillance.

Dans les pages qui suivent, nous examinons en effet l'hypothèse selon laquelle, loin de générer une domination explicite et écrasante, les pratiques sécuritaires contemporaines visent à développer des formes fluides et « adaptatives » de contrôle social. Ces pratiques brouillent les frontières traditionnelles entre la sphère publique et la sphère privée et nous invitent à repenser les régimes des droits fondamentaux en vigueur, notamment au regard de la tension entre impératifs de sécurité et protection de la vie privée et des données personnelles.

Au plan empirique, cet article se focalise sur les tendances qui émergent de la « stratégie européenne de sécurité intérieure » (SSI) ainsi que sur des mesures spécifiques proposées ou déjà approuvées au niveau européen [Conseil européen, 2010]. Une attention particulière est accordée à la proposition de la Commission européenne concernant la mise en place d'un système européen de collecte et de traitement des dossiers passagers, mieux connu sous l'acronyme anglais PNR (*Passenger Name Record*) [2011b]. En effet, cette mesure nous permet d'analyser comment les tendances identifiées dans la SSI sont traduites dans un dispositif politico-juridique visant à construire un espace à la fois dynamique et contrôlé.

1. LA SÉCURITÉ INTÉRIEURE EUROPÉENNE OU L'EUROPE FACE À SES CITOYENS

La réalisation d'un « espace de liberté, de sécurité et de justice » au sein de l'Union européenne doit être appréhendée comme un grand projet mobilisateur, un projet éminemment politique, susceptible d'introduire dans le processus d'intégration européenne le dynamisme indispensable à sa perpétuation et à sa légitimation[1]. Tout comme la réalisation du marché unique ou la création de la monnaie unique dans les décennies précédentes, ce projet trouve sa place au sein d'un processus plus large visant à réconcilier les individus avec l'Europe et à créer, selon la formule consacrée, une « union sans cesse plus étroite entre les peuples »[2]. Dans cette perspective, le droit de circuler librement et en toute sécurité dans un espace sans frontières intérieures apparaît comme un attribut de la citoyenneté européenne [Mitsilagas *et al*., 2003, pp. 7-8]. Les États membres entendent démontrer ce faisant aux citoyens que l'Europe peut se manifester positivement dans leur vie quotidienne en étendant l'espace géographique au sein duquel la sécurité est assurée et les libertés publiques respectées. L'enjeu est rien moins que d'attester dans la vie quotidienne de chaque Européen de la formation d'un ordre politique européen et de la contribution effective des institutions de l'Europe à la sécurité individuelle et collective.

En s'engageant sur la voie de la sécurité intérieure européenne, l'UE s'ouvre un accès privilégié à un réservoir de légitimation considérable. Elle ouvre également la boîte de Pandore. Car si l'implication des institutions européennes dans le champ de la sécurité est un ressort de la légitimation politique [Duez, 2008b], elle apparaît pour le moins risquée. Le triptyque « liberté, sécurité, justice » rompt en effet avec la conception technocratique de la légitimité sur laquelle a longtemps reposé l'intégration européenne [Magnette, 2003, pp. 25-34]. Il active à l'inverse une dynamique de justification plus classique articulant, d'une part, l'offre publique de sécurité et, d'autre part, la demande de protection des citoyens. La difficulté réside ici dans le fait que les fonctions régaliennes qui constituent le domaine central de l'action de la puissance publique n'ont été que très partiellement affectées par la construction européenne. À certains égards, le discours sur l'ELSJ – aussi fondamental soit-il en ce qu'il bouleverse les schémas conceptuels en vigueur depuis la naissance de l'État-nation – reste largement déconnecté de toute action concrète. S'il existe bien une ébauche de parquet européen (Eurojust), le germe d'un hypothétique corps de douane communautaire (Frontex) ou encore une structure de la collaboration policière (Europol), ces nouveaux instruments ne sont rien en regard des besoins ou de l'ambition affichée dans les discours européens. Cette faiblesse apparaît d'autant plus importante que ces organes ne sont, apparemment, que des mises en commun de moyens nationaux dont les États membres restent maîtres à chaque instant. L'Europe n'a à sa disposition, en propre, ni policiers, ni douaniers, ni cours et tribunaux ordinaires, ni administrations d'exécution.

En l'absence de moyens coercitifs propres, l'UE se trouve confrontée au dilemme suivant : comment répondre aux attentes suscitées auprès des citoyens européens avec les ressources qui sont les siennes ? Comment concilier les formidables ambitions du dis-

[1] Sur les déficits démocratique et de légitimité, ainsi que sur les différences entre ces deux concepts, voir Quermonne [2001, pp. 13-28] et Magnette [2000, pp. 173-198]. Pour une réflexion sur le rôle de la politique européenne de sécurité intérieure dans ces domaines, voir Duez [2008c].

[2] Cette expression était à l'origine la première phrase du préambule du traité de Rome. Elle a depuis traversé, quasiment intacte, toutes les étapes de la révision des traités.

cours communautaire en matière de sécurité intérieure et la volonté des États membres de garder intactes leurs prérogatives régaliennes ? Ce nœud politique est l'un des défis auquel l'Europe est aujourd'hui confrontée. Qu'elle parvienne à le résoudre en répondant aux attentes qu'elle a nourries et sa légitimité s'en verrait durablement établie. Qu'elle échoue et son action dans le champ de la sécurité, loin de contribuer à combler son déficit de légitimité, risquerait au contraire de l'aggraver [Duez, 2008c].

2. LE *POLICING* COMME NOUVEAU CONTRÔLE SOCIAL

Face à ce dilemme, certains éléments semblent jouer en faveur de l'UE. Historiquement affaire de police et de justice pénale, les politiques de sécurité tendent en effet à se transformer, accordant une place croissante à l'échange et aux traitements de l'information, et ce, au détriment des formes plus traditionnelles de la coercition. Cette évolution offre à l'Union une place de choix dans un paysage européen de la sécurité intérieure en recomposition. Dans une perspective du temps long, c'est en réalité la vision wébérienne de l'autorité politique qui se voit en partie remise en cause par une double transformation : d'une part le rejet progressif de la violence physique – tant individuelle qu'étatique – hors de l'espace public et, d'autre part, le passage d'une gestion essentiellement répressive de la sécurité publique vers des formes plus douces de contrôle social.

Concernant la première évolution, Norbert Elias a notamment montré comment s'est opéré le passage de la contrainte sociale à l'autocontrainte, c'est-à-dire l'intériorisation progressive et de moins en moins consciente de normes de comportement [1990]. Entre le 12ème et le 18ème siècle, les sensibilités se seraient profondément modifiées en Europe. Tandis que la division des fonctions accentuait la dépendance fonctionnelle entre les différentes couches de la population et favorisait, chez chaque individu, un plus grand contrôle de son comportement et de ses réactions pulsionnelles, la monopolisation par l'État de la violence a quant à elle accentué ce processus en sanctionnant par le droit ces évolutions comportementales [1990, p. 192]. En retour, cette limitation de la violence interpersonnelle a rendu possible, selon Elias, la réduction progressive du recours à la coercition par l'autorité politique. Dans les sociétés démocratiques, l'usage de la violence par les forces de l'ordre répond en effet à un principe de retenue [Garapon, 1998]. L'enjeu devient celui de la conservation de l'ordre établi par l'utilisation de méthodes modérées de coercition visant à épargner le coût élevé du rétablissement de l'ordre. Le processus de démocratisation s'est ainsi accompagné d'une aspiration croissante à maintenir un état de paix et de liberté tout en évitant de montrer une violence qui, en cas de répression désordonnée, pourrait discréditer les fondements politiques du régime [Bruneteaux, 1996, p. 25].

Analytiquement, cette double évolution correspond au passage de la logique de la police à celle du *policing*, qui désigne « un complexe dynamique d'activités de régulation de désordres, soutenus par des agents publics, privés, hybrides au sein de différents niveaux d'organisation sociopolitique territorialisés : microlocal, local, régional, national, supranational » [Ocqueteau, 2004, p. 50]. En d'autres termes, le *policing* est un ensemble de pratiques qui visent à ordonner les populations humaines qui habitent ou traversent un espace ou un territoire donné tout en conservant simultanément le contrôle de cet espace ou de ce territoire et de ceux qui l'occupent [Sheptycki, 2005, p. 29]. Les pratiques de sécurité reposeraient sur une articulation plus subtile des moyens répressifs et des techniques de contrôle social, en lien avec l'objectif actuel de combiner les impératifs de sécurité et de liberté.

Au plan opérationnel, la notion de *policing* suppose plusieurs évolutions. Premièrement, elle souligne le rôle des pratiques de surveillance ainsi que l'importance croissante des processus d'identification et d'évaluation des dangers dans les politiques de sécurité. En cela, le *policing* prolonge la révolution identificatoire, mise en évidence par Gérard Noiriel, qui s'était caractérisée par l'identification de l'ensemble des individus présents sur le territoire d'un État et par l'introduction des documents d'identité [1998]. Plus largement, cette pratique s'inscrit dans le prolongement du projet consistant, depuis le 17ème siècle, à enserrer la gestion de populations entières dans un ensemble de techniques, de procédés, de savoirs, de descriptions statistiques et de recettes empiriques visant à les rendre plus dociles aux exigences du système urbain et industriel [Berges, 1988, p. 335 ; Berns, 2009]. Ce nouvel art de gouverner s'est développé initialement dans le contexte des doctrines de la raison d'État [Lazzeri & Reynié, 1992 ; Sfez, 2000] – au sens de Giovanni Botero et de la *gute Polizei* allemande – avant d'être conceptualisé par Michel Foucault au travers des notions de « biopouvoir », « biopolitique » ou encore de « gouvernementalité » [1976, 2004]. Dans le champ de la sécurité, cet art de gouverner s'est historiquement appuyé sur une série de technologies, comme la phrénologie, la photographie judiciaire ou, plus récemment, la construction de profils biométriques [Mattelart, 2008, pp. 13-28]. S'exprime ainsi une croyance dans la capacité des autorités publiques à veiller à la préservation de l'ordre social par le recours aux outils de la science et de la technique.

Deuxièmement, la notion de *policing* traduit un passage de la gestion des désordres publics à la gestion des risques sociaux. La construction d'un savoir positif sur l'organisation du corps social autorise en effet les acteurs de la sécurité à faire état d'une prétention croissante à la prévention des désordres. Il s'agirait désormais de contrôler la criminalité et la délinquance avant même leur irruption par la construction de profils-types, par l'identification des situations et lieux « à risque » ou encore par le recours généralisé aux pratiques de surveillance (caméra vidéo, biométrie, échanges formels et informels d'informations entre services de sécurité, etc. *cf. in extenso* Lyon [2007]). Outre les questions qu'elle soulève tant au plan de sa validité réelle que de la protection des droits fondamentaux, cette prétention induit un changement de paradigme : l'on passe de la logique de la répression à celle, non pas de la prévention, mais bien du contrôle, voire de la suspicion.

Enfin, troisièmement, la notion de *policing* suppose une reconfiguration du rapport à l'espace et au territoire. Cette notion brouille en effet tout aussi bien les relations entre les secteurs privés et publics, en impliquant les acteurs privés de la sécurité dans la gestion des affaires publiques, que les limites géographiques des États-nations. Le *policing* est par nature transnational. Guidées par la seule logique de son efficacité, les nouvelles politiques de sécurité s'émancipent des carcans nationaux et s'ouvrent à la formalisation des coopérations entre les services de police et de justice nationaux ou infra-nationaux.

3. PRIVILÉGIER L'ANTICIPATION ET LA PRÉVENTION : LE CAS DES PNR[3]

La « stratégie européenne de sécurité intérieure » (SSI), approuvée par le Conseil européen en mars 2010, s'inscrit pleinement dans la logique des évolutions qui viennent d'être décrites [Conseil européen, 2010]. Confirmant le lien étroit entre citoyenneté, légitimation de l'UE et offre publique de sécurité, le texte pose tout d'abord que :

[3] *Passenger Name Record*.

> La qualité de notre démocratie et la confiance publique à l'égard de l'Union dépendront dans une large mesure de notre capacité à garantir la sécurité et la stabilité en Europe et du travail effectué avec nos voisins et partenaires pour s'attaquer aux racines des problèmes que rencontre l'UE en matière de sécurité intérieure [Conseil européen, 2010, p. 9].

Il identifie ensuite les principales menaces affectant les Européens. Surtout, la SSI pose les bases d'un « modèle européen de sécurité » intégrant les stratégies et approches conceptuelles existantes, et notamment celles figurant dans le programme de Stockholm – au nom très évocateur : « Une Europe ouverte et sûre qui sert et protège les citoyens » [Conseil européen, 2009] – et le plan d'action visant à sa mise en œuvre [Commission européenne, 2010b]. La stratégie insiste en particulier sur la nécessité de privilégier une action « en amont » fondée sur le renseignement. Prévention et anticipation sont ici les maîtres mots :

> La prévention et l'anticipation, en matière de criminalité, mais aussi en ce qui concerne les catastrophes naturelles ou anthropiques et l'atténuation de leur impact potentiel figurent parmi les objectifs principaux de la stratégie de sécurité intérieure de l'UE. Certes, il demeure essentiel de poursuivre efficacement les auteurs d'infractions ; néanmoins mettre davantage l'accent sur la prévention d'actes criminels et d'attentats par une action en amont peut contribuer à réduire les préjudices humains ou psychologiques causés par de tels actes, qui sont souvent irréparables [Conseil européen, 2010, p. 22].

Les politiques de sécurité doivent par conséquent englober les services de maintien de l'ordre mais aussi des établissements et des professionnels intervenant au niveau national et local, tant dans le secteur public que privé. Ces politiques doivent en outre reposer sur la confiance mutuelle et le principe générique de la mise à disposition des informations. Prévenir la menace suppose donc d'agir « à la source » en matière de sécurité [Conseil européen, 2010, p. 24]. Dans ce but, les services de sécurité devraient avoir accès en temps utile à toutes les données susceptibles de concerner les activités criminelles, leurs auteurs et leurs modes opératoires, la typologie des victimes, etc. Or, pour permettre et faciliter cet accès, il est nécessaire d'assurer un stockage continu des données, soit auprès d'institutions publiques spécifiques, soit auprès d'institution privées (comme les opérateurs des télécommunications), et, dans les deux cas, soit de manière centralisée (dans une seule base de données), soit de manière décentralisée.

Loin de se limiter aux cas de criminalité avérée, les données collectées concernent aussi de simples citoyens européens ou des ressortissants de pays tiers. S'inspirant de l'expérience américaine en ce domaine[4], la SSI reprend ainsi l'idée d'un système européen de traitement des dossiers des passagers, ou PNR [Conseil européen, 2010, pp. 23-4]. Ce projet a depuis fait l'objet d'une proposition de directive présentée par la Commission en février 2011 [2011b][5]. Cette mesure, encore au stade de projet, est particulièrement intéressante pour notre recherche parce qu'elle suppose un traitement massif et indiscriminé de données personnelles [Bellanova & Duez, 2012].

Concrètement, les dossiers passagers contiennent des données demandées par une compagnie aérienne lors de l'achat d'un billet, c'est-à-dire des données avant tout commerciales. Historiquement, les systèmes PNR ont en effet été conçus pour assurer la gestion des réservations d'un nombre grandissant de voyageurs et, de plus en plus, pour répondre à la volonté des compagnies

[4] Pour une présentation critique des trois premiers accords touchant aux transferts des PNR au *Department of Homeland Security* des États-Unis, voir Papakonstantinou & De Hert [2009].

[5] Un premier projet de décision-cadre pour la mise en place d'un système PNR européen avait été déjà avancé en 2007.

aériennes d'offrir un service personnalisé à leurs passagers. Ces informations peuvent inclure non seulement les données biographiques et de contact, mais aussi des informations sur le paiement et les exigences ou préférences personnelles[6]. Ces données révèlent bien souvent des informations relatives aux pratiques religieuses ou à la situation médicale des voyageurs, c'est-à-dire des données sensibles soumises à un régime de protection renforcée dans la plupart des États membres de l'UE.

Collectées à l'origine à des fins commerciales, ces données PNR peuvent être utilisées dans le cadre des politiques de sécurité. Cet usage suppose toutefois un traitement spécifique d'une information qui n'a, sous sa forme brute, aucune signification. Pour devenir signifiantes, les informations collectées doivent passer par le filtre de technologies d'analyses complexes. Dans le cas du projet PNR européen, ce filtrage devrait être opéré par des « unités de renseignement passagers » à instituer au niveau national [Commission européenne, 2011b, art.3-4]. Trois formes de traitement sont explicitement mentionnées :

1. un mode réactif,
2. un mode en temps réel et
3. un mode proactif [Commission européenne, 2011b, pp. 4-7, et art. 4]. Dans le premier mode, les données PNR seraient utilisées pour reconstruire *ex post* les déplacements et les relations avec des tiers de personnes interceptées par les forces de l'ordre ou poursuivies par la justice. Ce mode fonctionnerait « au cas par cas, aux demandes dûment motivées d'autorités compétentes visant à obtenir des données PNR et le traitement de celles-ci dans des cas spécifiques » [Commission européenne, 2011b, art.4(c)]. Dans le cadre de la deuxième forme de traitement, les PNR seraient comparées à des bases de données préétablies par des agences de police et de sécurité pour identifier des terroristes et de criminels qui sont déjà connus des autorités. Les PNR seraient également confrontés à des « critères d'évaluation préétablis afin d'identifier les suspects jusqu'alors « inconnus » [Commission européenne, 2011b, p. 4]. Cette analyse s'effectuerait en temps réel, avec la double ambition d'intervenir très tôt (avant le départ ou l'arrivé du vol concerné) et sur des « inconnus ». Si l'approche en temps réel vise déjà la prévention, ces deux premiers modes de traitement resteraient cependant des formes relativement « traditionnelles » de traitement des données personnelles. À ce titre, elles sont considérées comme des mesures de portée secondaire au regard de la richesse en information d'un dossier passager.

Le troisième mode de traitement, le traitement préventif, apparaît nettement plus novateur. Plus encore que le traitement en temps réel, il témoigne de l'ambition de détecter les terroristes et les criminels « inconnus » par l'entremise d'une évaluation du niveau de risque représenté par chaque passager [Commission européenne, 2011b, p. 7]. Ce troisième mode de traitement incarne ce « rêve de gouvernance ciblée », pour emprunter l'expression de Valverde et Mopas [2004]. Les PNR seraient ici utilisés pour « l'analyse et la définition de critères d'évaluation qui peuvent ensuite être appliqués afin d'évaluer le risque que représentent les passagers avant leur arrivée et avant leur départ » [Commission européenne, 2011b, p. 4]. Ainsi, les comportements, les préférences, les trajectoires des voyageurs seraient utilisés, *via* leur double inscription commerciale et sécuritaire, pour alimenter, améliorer et façonner le dispositif de contrôle.

Même si le texte de la Commission opte pour le terme relativement neutre d'évaluation du risque, ces deux derniers modes de traitement des PNR, s'ils venaient à être mis en œuvre, introduiraient *de facto* un système de *data mining* et de *profiling* à échelle européenne.

[6] Par ailleurs, toutes les informations citées sont incluses dans la liste annexée au projet de directive [Commission européenne, 2011b, p. 35].

Ces technologies d'analyse consistent en effet en un ensemble de techniques automatisées utilisées pour extraire des renseignements enfouis ou inconnus jusque-là de grandes bases de données [Cavoukian, 1998, p. 4]. Une extraction de données réussie permet ainsi, au départ de grandes bases de données, de mettre au jour des modèles et des relations, et d'utiliser ensuite ces nouvelles informations pour prendre une décision basée sur la connaissance proactive [Cavoukian, 1998, p. 4]. Il s'agirait en l'espèce d'identifier des suspects, de détecter des activités illégales et de prévenir les menaces. Dans cette optique, l'extraction de données n'adopte pas une approche hypothético-déductive (celle de la vérification) mais une approche inductive (celle de la découverte) [Berns & Rouvroy, 2010b, pp. 91-92]. Si la première approche se base sur la formulation d'une hypothèse, par exemple la relation entre deux actions, qui est ensuite vérifiée ou rejetée, la seconde n'implique pas en revanche la formulation d'une hypothèse. Elle permet d'examiner simultanément plusieurs relations de données multidimensionnelles en identifiant celles qui sont uniques ou au contraire récurrentes.

Loin d'être un cas isolé, le développement du système PNR européen apparaît révélateur des évolutions à l'œuvre dans le champ de la sécurité intérieure européenne. Le renforcement des échanges d'informations et la digitalisation des données peut en effet s'observer dans de nombreux domaines. Au fil des ans, les fichiers se sont en effet multipliés. Citons simplement le système d'information Schengen (SIS), le système d'information sur les visas (VIS), le système européen d'archivage d'image (FADO, « *False and Authentic Documents* »), la base de données EURODAC de comparaison des empreintes digitales des demandeurs d'asile et des immigrants clandestins, le fichier d'identification des dossiers d'enquêtes douanières (FIDE), le système de gestion de cas de l'Office de la lutte antifraude (OLAF) et d'Eurojust, le système d'information douanier (SID), le système d'information Europol (SIE), les fichiers d'analyses de risques de Frontex, le système informatique antifraude de l'OLAF (AFIS), le système européen automatisé d'identification criminelle des empreintes digitales (AFIS-D) et, enfin, les fichiers d'index et d'analyse d'Europol [Commission européenne, 2010c].

Comme le montre la liste ci-dessus, c'est dans les domaines de la gestion des frontières extérieures que le développement de pratiques sécuritaires nouvelles se révèle le plus frappant. Dans ce contexte centré sur le suivi des individus et de leurs déplacements, la mise en place d'un espace européen sous contrôle passe bien souvent par l'usage de la biométrie aux fins de sécurisation des documents de voyage. Cet usage suppose la collecte et le stockage d'une quantité toujours plus importante de données relatives aux caractéristiques physiques des individus. Il se traduit également par la mise en circulation de documents électroniques standardisés permettant l'échange de ces données entre les services compétents des États membres et, sous certaines conditions, avec les services d'États tiers.

Plus spécifiquement, sans en être explicitement une composante, le projet PNR européen rejoint la logique du projet de gestion intégrée des frontières extérieures de l'UE (ou *integrated border management* – IBM) mis en œuvre depuis de l'adoption du « paquet frontières » présenté par la Commission en 2008 (révisé en 2011). Le projet IBM affiche en effet l'ambition de créer des « frontières intelligentes » en renforçant le prisme de la technologisation de la sécurité [Commission européenne, 2008b ; 2011a]. Parmi les différents dispositifs prévus par la Commission dans le cadre du projet IBM, le programme d'enregistrement des voyageurs (RTP) apparaît particulièrement en phase avec le système PNR[7]. Dans un futur

[7] Parmi les autres projets signalons le système d'enregistrement des entrées et sorties du territoire de l'UE des ressortissants de pays tiers admis pour un séjour inférieur à trois mois, le système électronique d'autorisation de voyage (ESTA) ou encore le système de surveillance électronique des frontières (EUROSUR) [Commission européenne, 2008a, 2011c].

proche, le RTP devrait en effet permettre aux individus intéressés de s'inscrire dans un registre de voyageurs *bona fide*, moyennant un contrôle préliminaire et le paiement d'un abonnement. L'enregistrement au programme réduirait ensuite les lourdeurs des contrôles aux frontières pour les personnes enregistrées.

4. L'ENJEU DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Développés dans le cadre de la lutte contre l'immigration clandestine et du contrôle des mobilités transfrontalières, les dispositifs évoqués ci-dessus incarnent les nouvelles manières de faire la sécurité. Ils sont à l'origine d'un quadrillage qui tend à couvrir l'ensemble du corps social. À la faveur de l'élargissement de ces fichiers, de leur interconnexion croissante et de l'assouplissement des conditions de consultation des informations par les divers corps de l'État ou agences européennes, on observe une multiplication des lieux et des occasions de contrôle au sein d'un espace pourtant réputé sans contrôle aux frontières. Ce contrôle apparaît toutefois de moins en moins visible et de moins en moins sensible pour les individus dont la mobilité aura été préalablement considérée comme légitime. Il se fait à l'inverse de plus en plus contraignant et pesant pour certaines populations identifiées comme indésirables [Duez, 2008a]. Cette tentative de distinguer les voyageurs légitimes (*bona fide travellers*) des voyageurs illégitimes (*mala fide travellers*) qu'il convient d'intercepter, le dispositif mis en place n'est pas sans effet sur le citoyen européen ou le simple voyageur.

Souvent représentée comme une pure question « technique », « non politique » et « inoffensive » pour les citoyens, la politique de sécurisation par les fichiers est généralement justifiée par son apparente « bénignité » [Berns & Rouvroy, 2010b]. Selon Berns et Rouvroy : « il s'agit toujours 'seulement' de gouverner dans un sens qui apparaîtrait évident et justifié par le sens commun, c'est-à-dire nécessairement bénin pour ceux qui sont gouvernés, tel est le fond de légitimité du gouvernement statistique » [2010a]. Légitimée par les fins qu'elle poursuit, la surveillance électronique le serait également en raison de son caractère indifférencié. Le caractère virtuellement infini des capacités de stockage et la diminution corrélative du coût des mémoires digitales facilement interconnectées auraient favorisé la « banalisation » de la surveillance. Devenue « démocratique et égalitaire », elle ne prétendrait plus cibler personne *a priori*, mais s'appliquerait à tout le monde par défaut [Berns & Rouvroy, 2010b, p. 90]. Toute forme de réticences et de résistances s'en trouverait disqualifiée par avance. L'argument suivant lequel « qui n'a rien à cacher n'a rien à craindre de la surveillance » l'emporterait largement sur la réticence au dévoilement de la vie privée et de l'intimité, d'autant que l'effacement de ses traces digitales demande, de la part de l'individu, une démarche active tandis que leur conservation se fait par défaut.

Cette banalisation de la surveillance caractérisée par un certain degré d'acceptation de la part des surveillés, voire par leur participation active à cette surveillance, ne suffit pas à évacuer toute préoccupation en matière de protection des droits fondamentaux des citoyens européens [Bellanova *et al*., 2010]. Au contraire, combinée à la multiplication et au renforcement de la surveillance, l'inconscience des surveillés la rend plus essentielle encore. De manière significative, les questions du droit à la vie privée et de la protection des données à caractère personnel occupent d'ailleurs une place croissante dans le débat académique [Gutwirth *et al*., 2009] mais aussi sur la scène politique européenne, allant jusqu'à la création, en 2001, d'une nouvelle institution : le Contrôleur Européen de la Protection des Données (CEPD).

La stratégie européenne de sécurité intérieure évoquée plus haut pose ainsi comme premier principe directeur du modèle européen de sécurité que la justice, la liberté et la sécurité sont « des politiques complémentaires, qui respectent les droits fondamentaux, l'accès à la protection internationale, l'État de droit et la vie privée » [Conseil européen, 2010, p. 19]. De pareilles références se retrouvent également dans le programme de Stockholm qui consacre un point à la protection des droits du citoyen dans une société de l'information [Conseil européen, 2009, pp. 18-19]. Ces déclarations paraissent cependant bien faibles au regard de l'investissement européen massif dans les technologies de surveillance et d'échange de données à caractère personnel, notamment pour la mise en œuvre de la SSI [Commission européenne, 2010a]. Et, de fait, le CEPD n'a pas manqué d'épingler ce dernier document en soulignant que plusieurs stratégies proposées dans le cadre de la SSI ont un impact direct ou indirect sur la protection des données à caractère personnel [JOUE, 2011a]. Dans le même registre, d'autres opinions émises par le CEPD, notamment sur le dossier des PNR européens évoqué plus haut, réitèrent cette inquiétude latente à l'égard de la collecte et du traitement des données personnelles à des fins sécuritaires [JOUE, 2011b]. Au premier rang de ces inquiétudes, on retrouve le caractère parcellaire et peu cohérent de la législation européenne en matière de protection des données utilisées à des fins de sécurité.

Au niveau européen, la protection de la vie privée et la protection de données personnelles reposent en effet sur un *patchwork* d'instruments juridiques. Par ailleurs, si la vie privée (*privacy*) et la protection des données personnelles (*data protection*) sont souvent considérées comme des synonymes, leur relation est complexe, tant d'un point de vue juridique que philosophique. Au plan des sources juridiques, l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) de 1950 et l'article 7 de la Charte des droits fondamentaux de l'Union européenne de 2000 fournissent les principaux instruments juridiques au fondement de la protection de la vie privée. La protection des données personnelles se fonde quant à elle (entre autres) sur la Directive Protection des Données Personnelles [JOCE, 1995], sur la Décision-Cadre concernant la protection des données personnelles en matière de coopération policière et judiciaire [JOUE, 2008], et sur la Convention n° 108 du Conseil de l'Europe [Conseil de l'Europe, 1981]. Plus récemment, la protection des données personnelles s'est vue reconnaître une place spécifique dans le Traité sur le fonctionnement de l'UE (art.16) et a obtenu le statut formel de droit fondamental avec l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

En dépit de cette abondante législation, le cadre législatif européen apparaît encore plus complexe lorsqu'on l'examine sous l'angle des politiques de sécurité. La directive relative à la protection des données de 1995 ne s'applique par exemple pas au traitement des données à caractère personnel ayant pour objectif la sécurité publique, la défense, la sûreté de l'État […] et les activités de l'État relatives à des domaines du droit pénal » [JOCE, 1995, art.3(2)]. De même, elle ne s'applique pas non plus au traitement des données collectées d'abord par des acteurs privés et auxquelles on accède ensuite à des fins de sécurité publique, ce qui est le cas des PNR [Cour de Justice, 2006]. Pour ce qui concerne l'échange de données entre les services répressifs, tant au niveau européen qu'international – domaine en pleine expansion –, le cadre législatif offert par la Décision-Cadre n'est pas considéré approprié, et il est souvent compensé par l'adoption de dispositions *ad hoc* de protection des données dans les textes concernés. Cette approche prévaut par exemple dans la proposition de directive européenne sur les PNR qui inclut des sauvegardes de protection de données personnelles [Commission européenne, 2011b, art.11]. Ce modèle protectionnel soulève pourtant une tension : d'un côté, des mesures *ad*

hoc peuvent garantir une protection plus appropriée face au système technologique proposé mais, de l'autre, elles peuvent introduire des véritables exceptions aux principes généraux de la protection de données personnelles, et tendent à affaiblir la cohérence du cadre de protection général. Les débats concernant la nécessité ou l'utilité d'un cadre législatif à la fois exhaustif et homogène dans ce domaine ont été relancés récemment, avec une nouvelle proposition de directive concernant la protection des données utilisées à des fins sécuritaires [Commission européenne, 2012].

Au plan philosophique, Stefano Rodotà souligne que le droit au respect de la vie privée et familiale est avant tout le reflet d'une préoccupation individualiste. À l'inverse, la protection des données définit des règles et des mécanismes de traitement des données et donne à chacun la possibilité d'agir. Le premier droit est statique et négatif tandis que le second est dynamique : il suit les éléments d'une donnée dans tout leur parcours [Rodotà, 2010, p. 58]. De plus, dans le second cas, le contrôle n'est pas laissé aux seuls sujets mais aussi confié à une autorité indépendante qui en porte la responsabilité. Pour Rodotà, il s'agit là d'une redistribution des pouvoirs sociaux et légaux [2010, p. 58]. De manière similaire, Paul De Hert et Serge Gutwirth ont montré que le processus de différentiation entre vie privée et protection des données personnelles est propre à « l'histoire et la pratique des États constitutionnels démocratiques » et, en particulier, « à l'usage et à l'articulation de deux différents instruments constitutionnels ou légaux » [2008, p. 275 (traduction des auteurs)]. Il y a ainsi, d'un côté, les instruments « qui visent à garantir la non-interférence dans les questions individuelles et l'opacité (*sic*) de l'individu » et, de l'autre côté, les instruments « qui visent à organiser et garantir la transparence et l''*accountability*' du puissant » [Idem].

Sous cet angle, la protection de la vie privée et la protection des données personnelles apparaissent comme des enjeux importants dans les relations de pouvoir entre les citoyens et les agences de sécurité, de plus en plus marquées par la technologie et l'usage des informations personnelles. Une citoyenneté active passe aujourd'hui, entre autres, par des mécanismes juridiques et discursifs liés à ces deux droits, comme la possibilité d'ester en justice, de « problématiser » un traitement de données personnelles, d'introduire des obstacles technologiques ou des filtres, à l'accès, au stockage ou au traitement de ces données, ou encore de négocier une limitation du contrôle, sinon sa désactivation.

CONCLUSION

Parce qu'elle ne dispose pas comme les États membres d'organes spécialisés exerçant au nom de l'autorité politique une coercition légitime sur les individus déviants, l'UE s'est engagée sur une voie alternative pour déployer sa politique de sécurité intérieure et renforcer sa relation avec les citoyens. Elle a choisi d'exploiter les potentialités des nouvelles technologies de l'information et de la communication pour développer un modèle de sécurité intérieure fondé sur l'élaboration d'un modèle global pour l'échange d'informations qui privilégie la prévention et l'anticipation. Ce faisant, l'Union s'inscrit largement dans un processus socio-historique caractérisé par un recours accru aux techniques de contrôle social dans le domaine des politiques de sécurité et pour la gestion des espaces et des populations.

Ce passage d'une logique de la police à celle du *policing* soulève cependant de nouveaux enjeux en matière de protection des droits fondamentaux des citoyens. Ces nouveaux modes de gouvernance sécuritaire ne génèrent plus forcément les mêmes types de

problèmes que ceux associés classiquement au maintien ou au rétablissement de l'ordre. La violence policière, la détention abusive ou le procès arbitraire n'apparaissent plus ici comme les principales formes de l'atteinte aux droits des individus. À l'heure de la technologisation du contrôle social, si la pratique sécuritaire est digitalisée et apparemment dématérialisée, il en va de même des violations des droits fondamentaux. Ce sont désormais les enjeux de la protection de la vie privée et de la protection des données personnelles qui apparaissent primordiaux.

Les mutations que nous avons analysées dans le champ de la sécurité intérieure européenne nous semblent également révélatrices d'une évolution de la relation gouvernants-gouvernés. Dans le modèle de la « société de police », le pouvoir tend à assujettir les individus par la norme, à les rendre dociles, c'est-à-dire conformes aux valeurs et comportements définis comme bons par la société. À l'inverse, le gouvernement par les fichiers ne cherche pas *a priori* à infléchir les comportements des citoyens. La logique statistique sous-jacente suppose au contraire, pour être efficace, que chaque individu continue à agir normalement – c'est-à-dire « à sa manière » – indépendamment du dispositif de surveillance auquel il est soumis. C'est ici l'aberration ou du moins la particularité statistique qui permet de détecter les comportements à risque. Au lieu d'induire une discipline, le gouvernement par les fichiers est donc lui-même façonné par le réel et les comportements individuels, comme en témoignent les pratiques du *data mining* et du profilage.

Pour autant, les mécanismes de normalisation ne sont pas absents. Si la sécurité par la surveillance postule la stabilité des comportements des individus, elle induit dans la pratique, une adaptation des surveillés à la logique même de la surveillance. Chaque individu accepte en effet d'être surveillé et, par ce fait même, suit la voie plus classique de la disciplinarisation.

BIBLIOGRAPHIE

BELLANOVA R. *et al*. (2010), Variations sur le thème de la banalisation de la surveillance, *Mouvements*, n° 62, pp. 46-54.

BELLANOVA R. & DUEZ D. (2012), A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage, *European Foreign Affairs Review*, vol. 17, pp. 109-124.

BERGES M. (1988), « Michel Foucault et la police », *in* J.-L. Loubet Del Bayle (Ed.), *Police et société*, Toulouse, Presses de l'Institut d'études politiques de Toulouse, pp. 315-352.

BERNS T. (2009), *Gouverner sans gouverner. Une archéologie politique de la statistique*, Paris, PUF.

BERNS T. & ROUVROY A. (2010a), « Détecter et prévenir : de la digitalisation des corps et de la docilité des normes », *in* G. Lebeer & J. Moriau (Éds), *(Se) gouverner. Entre souci de soi et action publique*, Bruxelles, P.I.E. - Peter Lang, pp. 157-184.

BERNS T. & ROUVROY A. (2010b), Le nouveau pouvoir statistique. Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps 'numériques'…, *Multitudes*, n° 40, pp. 88-103.

BRUNETEAUX P. (1996), *Maintenir l'ordre. Les transformations de la violence d'État en régime démocratique*, Paris, Presses de Sciences Po.

CAVOUKIAN A. (1998), *Data Mining: Staking a Claim on Your Privacy*, Toronto, Information and Privacy Commissioner of Ontario.

COMMISSION EUROPÉENNE (2008a), *Examen de la création d'un système européen de surveillance des frontières (EUROSUR)*, Bruxelles, Commission européenne.

COMMISSION EUROPÉENNE (2008b), *Préparer les prochaines évolutions de la gestion des frontières extérieures dans l'Union européenne*, Bruxelles, Commission européenne.

COMMISSION EUROPÉENNE (2010a), *La stratégie de sécurité intérieure de l'UE en action : cinq étapes vers une Europe plus sûre*, Bruxelles, Commission européenne.

COMMISSION EUROPÉENNE (2010b), *Mettre en place un espace de liberté, de sécurité et de justice au service des citoyens européens. Plan d'action mettant en œuvre le programme de Stockhol*m, Bruxelles, Commission européenne.

COMMISSION EUROPÉENNE (2010c), *Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice*, Bruxelles, Commission européenne.

COMMISSION EUROPÉENNE (2011a), *Frontières intelligentes : options et pistes envisageables. Communication de la Commission au Parlement européen et au Conseil*, Bruxelles, Commission européenne.

COMMISSION EUROPÉENNE (2011b), *Proposition de Directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière*, Bruxelles, Commission européenne.

COMMISSION EUROPÉENNE (2011c), *Proposition de règlement du Parlement européen et du Conseil portant création du système européen de surveillance des frontières (Eurosur)*, Bruxelles, Commission européenne.

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

CONSEIL DE L'EUROPE (1981), *Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, Conseil de l'Europe.

CONSEIL EUROPÉEN (2009), *Le programme de Stockholm – Une Europe ouverte et sûre qui sert et protège les citoyens*, Luxembourg, Journal officiel de l'Union européenne.

CONSEIL EUROPÉEN (2010), *Stratégie de sécurité intérieure pour l'Union européenne. Vers un modèle européen de sécurité*, Luxembourg, Office des publications de l'Union européenne.

COUR DE JUSTICE (2006), *Arrêt de la Cour (grande chambre) 30 mai 2006 dans les affaires jointes C-317/04 et C-318/04*, Luxembourg, Cour de Justice.

DE HERT P. & GUTWIRTH S. (2008), « Regulating Profiling in a Democratic Constitutional State », *in* M. Hildebrandt & S. Gutwirth (Eds), *Profiling the European Citizen. Cross Disciplinary Perspectives*, Dordrecht, Springer, pp. 271-291.

DELEUZE G. (1990), *Pourparlers*, Paris, Les Éditions de Minuit.

DUEZ D. (2008a), L'Europe et les clandestins : la peur de l'Autre comme facteur d'intégration ?, *Politique européenne*, vol. 26, pp. 97-119.

DUEZ D. (2008b), *L'Union européenne et l'immigration clandestine. De la sécurité intérieure à la construction de la communauté politique*, Bruxelles, Presses des Éditions de l'Université de Bruxelles.

DUEZ D. (2008c), « La 'crise' de l'Union et les apories de la sécurité intérieure européenne », *in* M. Dony & A. Weyembergh (Éds), *L'Union européenne : la fin, d'une crise ?* Bruxelles, Presses de l'Université de Bruxelles, pp. 69-84.

ELIAS N. (1990), *La dynamique de l'Occident*, Paris, Pocket.

FOUCAULT M. (1975), *Surveiller et punir : naissance de la prison*, Paris, Gallimard.

FOUCAULT M. (1976), *Histoire de la sexualité. Vol. 1. La volonté de savoir*, Paris, Gallimard.

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

GARAPON A. (1998), Que signifie maintenir l'ordre ?, *Esprit*, n° 248, pp. 125-126.

GUTWIRTH S. *et al*. [Eds] (2009), *Reinventing Data Protection?*, Dordrecht, Springer.

JOCE (1995), *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, Luxembourg, Journal officiel des Communautés européennes.

JOUE (2008), *Décision-Cadre 2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale*, Luxembourg, Journal officiel de l'Union européenne.

JOUE (2011a), *Avis du Contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen et au Conseil — « La stratégie de sécurité intérieure de l'UE en action : cinq étapes vers une Europe plus sûre »*, Luxembourg, Journal officiel des Communautés européennes.

JOUE (2011b), *Avis du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière*, Luxembourg, Journal officiel de l'Union européenne.

LAZZERI C. & REYNIÉ D. (1992), *La raison d'État : politique et rationalité*, Paris, Presses Universitaires de France.

LYON D. (2007), *Surveillance Studies. An Overview*, Cambridge, Polity Press.

MAGNETTE P. (2000), *L'Europe, l'État et la démocratie. Le souverain apprivoisé*, Bruxelles, Complexe.

MAGNETTE P. (2003), *Le régime politique de l'Union européenne*, Paris, Presses de Science Po.

MATTELART A. (2008), *La globalisation de la surveillance. Aux origines de l'ordre sécuritaire*, Paris, La Découverte.

MITSILAGAS V. *et al*. (2003), *The European Union and Internal Security. Guardian of the People?*, Basingtoke, Palgrave Macmillan.

NOIRIEL G. (1998), *Le Creuset français. Histoire de l'immigration, XIXe-XXe siècle*, Paris, Le Seuil.

OCQUETEAU F. (2004), *Polices entre État et marché*, Paris, Presses de Sciences Po.

OGIEN A. (2006), « Contrôle social », *in* S. Mesure & P. Savidan (Éds), *Le dictionnaire des sciences humaines*, Paris, PUF, p 205.

PAPAKONSTANTINOU V. & DE HERT P. (2009), The PNR Agreement and Transatlantic Anti-terrorism Cooperation: No firm human rights framework on either side of the Atlantic, *Common Market Law Review*, vol. 46, pp. 885-919.

QUERMONNE J.-L. (2001), *L'Europe en quête de légitimité*, Paris, Presses de Science Po.

RODOTÀ S. (2010), Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives, *Mouvements*, vol. 62, pp. 55-70.

SFEZ G. (2000), *Les doctrines de la Raison d'État*, Paris, Armand Colin.

SHEPTYCKI J. (2005), *En quête de police transnationale. Vers une sociologie de la surveillance à l'ère de la globalisation*, Bruxelles, De Boeck & Larcier.

VALVERDE M. & MOPAS M.S. (2004), « Insecurity and the Dream of Targeted Governance », *in* W. Larner & W. Walters (Eds), *Global Governmentality*, New York, Routledge, pp. 233-250.