D'une circulation à l'autre. Données des dossiers passagers et gouvernementalité numérique européenne

Bellanova, R.

Publication date
2018
Document Version
Final published version
Published in
La libre circulation sous pression

D'UNE CIRCULATION À L'AUTRE. DONNÉES DES DOSSIERS PASSAGERS ET GOUVERNEMENTALITÉ NUMÉRIQUE EUROPÉENNE

Rocco Bellanova (1)

Universiteit van Amsterdam (UvA) et Université Saint-Louis – Bruxelles (USL-B)

1. – Introduction

La libre circulation *et* sa régulation sont au cœur des politiques de l'Union européenne et, notamment, de la construction d'un Espace de liberté, de sécurité et de justice (ELSJ). Comme proclamé dans le traité sur l'Union européenne, cet espace se voudrait « sans frontières intérieures, au sein duquel est assurée la libre circulation des personnes, en liaison avec des mesures appropriées en matière de contrôle des frontières extérieures, d'asile, d'immigration ainsi que de prévention de la criminalité et de lutte contre ce phénomène » (2).

Les bases de données et les technologies numériques sont, au moins depuis la création du Système d'information Schengen (SIS) (3), parmi les instruments utilisés et mis à disposition par les institutions européennes pour favoriser la libre circulation et en prévenir les possibles

---

* Pour citer ce chapitre : R. Bellanova, « D'une circulation à l'autre. Données passagers et gouvernementalité numérique européenne », in H. Mercenier, E. Ni Chaoimh, L. Damay et G. Delledonne (éd.), *La libre circulation sous pression. Régulation et dérégulation des mobilités dans l'Union européenne*, Bruxelles, Bruylant, 2018, pp. 125-144.

(1) Cette recherche a bénéficié du support de l'Action de recherche concertée (ARC) « Why regulate? Regulation, de-regulation and legitimacy of the EU », financée par la Communauté française de Belgique, ainsi que du projet « *FOLLOW – Following the Money From Transaction To Trial* » (ERC-2015-CoG 682317), financé par l'*European Research Council* (ERC).

(2) Art. 3(2) Traité sur l'Union européenne (TUE). Voy. aussi le Titre V du Traité sur le fonctionnement de l'Union européenne (TFUE).

(3) Le SIS a été développé comme une « mesure compensatoire » à l'abolition des frontières intérieures entre les États participant à la Convention Schengen : Titre IV, Acquis de Schengen – Convention d'application de l'Accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, *JO*, L 239/19 du 22 septembre 2000. Voy. aussi E. Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden, Nijhoff, 2008 ; D. Broeders, « The new digital borders of Europe », *International Sociology*, vol. 22, n° 1, 2007, pp. 71-92.

effets négatifs (4). Ces systèmes informatiques, à travers la collection, le traitement et la « mise en circulation » des données personnelles, promettent de cibler les contrôles sur un petit nombre d'individus suspects. Ces technologies servent à la fois comme supports au contrôle des frontières extérieures et comme outils pour favoriser la coopération policière et judiciaire (5), les autorités des pays membres pouvant, par exemple, s'échanger des informations à travers des systèmes de communication.

Cette contribution vise à explorer les manières de gouverner la circulation des individus à travers la circulation des données personnelles, et notamment comment les institutions européennes mobilisent la protection des données personnelles pour façonner ce processus de numérisation. Ce chapitre se focalise sur le régime européen de collection et du traitement des données des dossiers passagers (en anglais : *Passenger Name Records* – PNR) à des fins de sécurité et d'enquête judiciaire, qui a été introduit en avril 2016, lors de l'adoption de la directive PNR (6).

Même si cet instrument législatif n'est pas, du point de vue strictement juridique, une mesure qui porte sur les contrôles de frontières (7), la directive PNR a des implications en lien avec la libre circulation parce

(4) L. Amoore, « Biometrics borders: governing mobilities in the war on terror », *Political Geography*, vol. 25, n° 3, 2006, pp. 336-351 ; T. Balzacq, « The policy tools of securitization: information exchange, EU foreign and interior policies », *Journal of Common Market Studies*, vol. 46, n°1, 2008, pp. 75-100 ; D. Bigo et E. Guild, (éd.), *Controlling Frontiers. Free Movement Into and Within Europe*, Aldershot, Ashgate, 2005 ; D. Broeders et J. Hampshire, « Dreaming of seamless borders: ICTs and the pre-emptive governance of mobility in Europe », *Journal of Ethnic and Migration Studies*, vol. 39, n° 8, 2013, pp. 1201-1218 ; E. Brouwer, « Data surveillance and border control in the EU: balancing efficiency and legal protection », in T. Balzacq et S. Carrera (éd.), *Security versus Freedom: A Challenge for Europe's Future*, Aldershot, Ashgate, 2006, pp. 137-154 ; H. Dijstelbloem et D. Broeders, « Border surveillance, mobility management and the shaping of non-publics in Europe », *European Journal of Social Theory*, vol. 18, n° 1, 2014, pp. 21-38 ; V. Mitsilegas, « Contrôle des étrangers, des passagers, des citoyens : surveillance et anti-terrorisme », *Cultures & Conflits*, vol. 58, 2005, pp. 155-182 ; J. Jeandesboz, « Smartening border security in the European Union: an associational inquiry », *Security Dialogue*, vol. 47, n° 4, 2016, pp. 292-309.

(5) L'article 77(1)(c) TFUE ainsi que l'article 87(2)(a) TFUE.

(6) Directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) 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, *JO*, L 119/132 du 4 mai 2016 (ci-après, « directive PNR »).

(7) Voy. le paragraphe 34 de la directive PNR. Depuis 2004, la transmission des données concernant l'identité des voyageurs est régie par la « directive API » qui « vise à améliorer les contrôles aux frontières et à lutter contre l'immigration clandestine, au moyen de la transmission préalable aux autorités nationales compétentes, par les transporteurs, de données relatives aux passagers », art. 1er de la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, *JO*, L 261/24 du 6 août 2004. Les données *Advance Passenger Information* (API) qui font l'objet de la directive API concernent l'identité des passagers telle qu'indiquée dans les documents utilisés par les voyageurs.

qu'elle vise à créer un système de surveillance de masse des passagers des vols entre l'Union européenne et un État tiers, et potentiellement aussi de certaines routes intra-UE (8). Il est prévu que les autorités nationales compétentes surveillent ces passagers aériens de manière numérique pour être en mesure d'identifier les individus suspects, afin de les sélectionner pour des contrôles plus approfondis et, le cas échéant, de procéder à leur arrestation avant l'embarquement dans l'avion. Toutefois, comme déclaré explicitement dans le texte de la directive PNR, la sécurité n'est pas l'unique objectif de cet instrument législatif : « [l]es objectifs de la présente directive sont, entre autres, d'assurer la sécurité, de protéger la vie et la sécurité des personnes, et de créer un cadre juridique pour la protection des données PNR en ce qui concerne leur traitement par les autorités compétentes » (9). L'ambition de cette directive est donc de façonner ce nouveau système de sécurité d'une manière telle qu'il puisse garantir la protection des données personnelles. Par ce biais, elle établit toute une série de pratiques qui accompagnent les opérations plus sécuritaires, comme l'identification des suspects parmi les passagers, et qui ont ainsi pour objectif l'aménagement de la circulation des données.

Le reste du chapitre se divise en quatre sections. La première section discute, de manière plus conceptuelle, comment les technologies de sécurité européennes s'inscrivent dans des dynamiques politiques et comment elles posent aussi des nouvelles questions gouvernementales par rapport à la manière d'organiser non une, mais plusieurs formes de circulation (des individus et des données). Cette section invite ainsi à étudier la directive PNR comme une « fenêtre » sur l'évolution d'une « gouvernementalité numérique européenne ». La deuxième partie retrace brièvement l'histoire du traitement informatique des données des dossiers passagers, en récapitulant les étapes et les débats majeurs qui ont accompagné les ambitions gouvernementales européennes à propos de l'exploitation sécuritaire et la protection de ces données commerciales. La section suivante introduit plusieurs éléments clés de la directive PNR en montrant et en analysant la double ambition de ce programme de gouvernement : gouverner la circulation des passagers à travers les données et gouverner la circulation des données elles-mêmes. Cette partie souligne également le rôle attribué à la protection des données personnelles dans les efforts de construction d'une pratique de sécurité. *In fine*, les conclusions soulignent comment une

(8) Art. 1er et 2 de la directive PNR.
(9) Voy. le paragraphe 5 de la directive PNR.

perspective inspirée des « études de la gouvernementalité » peut enrichir les débats académiques sur la construction de l'ELSJ en invitant à considérer l'émergence des données personnelles en tant que véritable problème de gouvernement pour les institutions européennes.

2. – Technologies de sécurité, protection de données et gouvernementalité européenne

Comme toute « instrumentation » de l'action publique, les systèmes technologiques de sécurité participent à plusieurs opérations politiques (10). D'un côté, ils contribuent à traduire les objectifs juridico-politiques de l'ELSJ mentionnés plus haut dans des programmes apparemment plus atteignables que l'intégration supranationale des fonctions régaliennes des États membres. En effet, la construction politique et juridique de l'ELSJ reste sujette à de multiples tensions, et ceci nonobstant une progressive institutionnalisation de la coopération entre professionnels de la police et de la justice, la création de nouvelles agences européennes et les efforts de « communautarisation » des affaires intérieures et de la justice du traité de Lisbonne (11). Comparé, par exemple, aux conflits entre autorités nationales et institutions européennes concernant la gestion de la « crise des réfugiés » (12), le traitement des données personnelles est souvent considéré comme une source moins importante d'opposition ou d'impasse politique.

De l'autre côté, gouverner la circulation des données soulève des problèmes et requiert des solutions à la fois du point de vue technique et en matière de respect des droits fondamentaux (13). Même si les enjeux

(10) P. Lascoumes et P. Le Galès (éd.), *Gouverner par les instruments*, Paris, Presses de Sciences-Po, 2004, pp. 11-44 ; A. Amicelle, C. Aradau et J. Jeandesboz, « Questioning security devices: performativity, resistance, politics », *Security Dialogue*, vol. 46, n° 4, 2015, pp. 293-306.

(11) D. Bigo, « Un espace de liberté, de sécurité et de justice ? », in R. Dehousse (éd.), *Politiques européennes*, Paris, Les Presses de Sciences Po, 2009, pp. 331-352 ; M. Den Boer, « Police, policy and politics in Brussels: scenarios for the shift from sovereignty to solidarity », *Cambridge Review of International Affairs*, vol. 27, n° 1, 2014, pp. 48-65 ; S. Lavenex, « Justice and home affairs. Institutional change and policy continuity », in H. Wallace, M.A. Pollack et A.R. Young (éd.), *Policy-Making in the European Union. Seventh edition*, Oxford, Oxford University Press, 2015, pp. 367-387 ; J. Monar, « Setting the context: why EU institutions matter in justice and home affairs », in F. Trauner et A. Ripoll Servent (éd.), *Policy Change in the Area of Freedom, Security and Justice. How EU Institutions Matter*, London, Routledge, 2015, pp. 3-10 ; E.M. Uçarer, « The area of freedom, security, and justice », in M. Cini et N. Pérez-Solórzano Borragán (éd.), *European Union Politics. Fifth edition*, Oxford, Oxford University Press, 2016, pp. 281-294.

(12) Presidency of the Council, *Integrity of the Schengen Area*, Brussels, Council of the European Union, 2015.

(13) F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange*

concernant la protection de la vie privée et des données personnelles sont moins souvent portés devant l'opinion publique que les conflits concernant la réintroduction des contrôles des frontières, ils restent cependant au cœur des débats institutionnels et sociopolitiques (14). De plus, ils sont systématiquement pris en compte par les acteurs européens dans les différents programmes d'action (15) et ils ont été « institutionnalisés » avec la création, entre autres, d'autorités nationales de protection de la vie privée et du Contrôleur européen de la protection des données (CEPD) (16). En d'autres mots, le développement et la mise en place des systèmes de surveillance numérique requièrent tout un art pour « bien traduire » à la fois les ambitions en termes de sécurité des acteurs européens et les objectifs de promotion de la liberté et de la justice dans le cadre de l'ELSJ.

Les technologies de sécurité guidées par les données renvoient à un « imaginaire cybernétique » où les systèmes informatiques offriraient des leviers non tant pour assurer la « subordination » des individus, mais plutôt pour « programmer » la gouvernance de leurs mouvements et des éventuels contrôles personnalisés (17). Cet « imaginaire » opère

at EU-level, Berlin, Springer, 2012 ; E. Brouwer, *Digital Borders and Real Rights*, *op. cit.* ; E. Brouwer, « Data surveillance and border control in the EU », *op. cit.* ; P. De Hert et S. Gutwirth, « Privacy, data protection and law enforcement. Opacity of the individual and transparency of power », in E. Claes, A. Duff et S. Gutwirth (éd.), *Privacy and the Criminal Law*, Antwerp, Intersentia, 2006, pp. 61-104.

(14) A. Ripoll Servent, « Holding the European Parliament responsible: policy shift in the data retention directive from consultation to codecision », *Journal of European Public Policy*, vol. 20, n° 7, 2013, pp. 972-987 ; Y. Suda, « Transatlantic politics of data transfer: extraterritoriality, counter-extraterritoriality and Counter-terrorism », *Journal of Common Market Studies*, vol. 51, n° 4, 2013, pp. 772-788.

(15) Voy., p. ex., Commission européenne, *Le programme européen en matière de sécurité*, Strasbourg, 2015, et, auparavant, *Le programme de Stockholm – Une Europe ouverte et sûre qui sert et protège les citoyens*, *JO*, C 115/1-38 du 4 mai 2010.

(16) Au niveau de l'Union européenne, il y a une autorité (publique et indépendante) de protection de données personnelles dans chaque État membre en accord avec l'article 28 de la 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, *JO*, L 281/31 du 23 novembre 1995. La coopération européenne entre ces autorités nationales est institutionnalisée au sein du Groupe de travail de l'Article 29, une organisation *sui generis* qui trouve sa base juridique justement dans l'article 29 de la directive 95/46/CE. Le Contrôleur européen de la protection des données personnelles a été institué par l'article 1(2) du règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, *JO*, L 8/1 du 12 janvier 2001. Voy. aussi : C.J. Bennett et C. Raab, *The Governance of Privacy. Policy Instruments in Global Perspective*, Cambridge, The MIT Press, 2006, pp. 133-143; et H. Hijmans, « The European data protection supervisor: the institutions of the EC controlled by an independent authority », *Comm. M.L.R.*, vol. 43, n° 5, 2006, pp. 1313-1342.

(17) A. Supiot, *La Gouvernance par les nombres. Cours au Collège de France (2012-2014)*, Nantes, Institut d'études avancées de Nantes/Fayard, 2015, p. 48. Valverde et Mopas parlent notamment du « dream of targeted governance » : « *our particular present is dominated by a*

comme toile de fond dans plusieurs débats politiques concernant la mise en place d'un régime PNR. On le retrouve à la fois chez ceux qui l'ont proposé comme outil pour tracer les suspects inconnus et, en filigrane, dans les critiques portant sur son impact sur la vie privée des voyageurs. Par contre, une exploration du texte de la directive PNR, et en particulier des solutions concernant la protection des données personnelles, montre que gouverner par les PNR requiert aussi de réfléchir aux, et d'organiser les, manières de gouverner les données.

En effet, l'intérêt porté par plusieurs acteurs européens aux technologies numériques, que celui-ci concerne les outils de sécurité ou la protection des données personnelles, nous permet d'étayer la discussion académique engagée dans ce volume en nous intéressant à la gestion de la libre circulation à travers les données. Plusieurs travaux issus des études critiques de la sécurité se sont déjà penchés sur une analyse des modes et des outils de gouvernement qui guident une (in) sécuritisation de la circulation (18). Ils soulignent également le rôle d'un nombre toujours grandissant de « professionnels de la sécurité » et des technologies numériques (19), ainsi que les effets institutionnels et politiques de la gestion des flux (20). Une littérature juridique de plus en plus intéressée par les nouvelles technologies et la surveillance aborde ces enjeux en termes de droits fondamentaux, en lien en particulier avec les questions de la vie privée et de la protection des données personnelles (21). Le dialogue avec ces travaux peut être ultérieurement enrichi par la sociologie politique de l'international, qui nous invite à

utopian governance dream – a "smart", specific, side-effects-free, information driven utopia of governance that in policing circles takes the form of "intelligence-led policing" and in medical circles is known as "evidence-based medicine" », in M. Valverde et M.S. Mopas, « Insecurity and the dream of targeted governance », in W. Larner et W. Walters (éd.), *Global Governmentality*, New York, Routledge, 2004, pp. 233-250.

(18) T. Balzacq, « The policy tools of securitization », *op. cit.* ; B.J. Muller, *Security, Risk and the Biometric State. Governing Borders and Bodies*, London, Routledge, 2010 ; M.B. Salter, « Imagining numbers: risk, quantification, and aviation security », *Security Dialogue*, vol. 39, n^{os} 2-3, 2008, pp. 243-266.

(19) D. Bigo, « The (in)securitization practices of the three universes of EU border control: Military/Navy - Border guards/Police - Database analysts », *Security Dialogue*, vol. 45, n° 3, 2014, pp. 209-225 ; D. Bigo, « EU police cooperation: national sovereignty framed by European security? », in E. Guild et F. Geyer (éd.), *Security versus Justice? Police and Judicial Cooperation in the European Union*, Aldershot, Ashgate, 2008, pp. 91-108.

(20) D. Bigo et E. Guild, *Controlling Frontiers*, *op. cit.* ; J. Jeandesboz, « Smartening border security in the European Union », *op. cit.* ; M. de Goede, « The Swift affair and the global politics of European security », *Journal of Common Market Studies*, vol. 50, n° 2, 2012, pp. 214-230.

(21) V. Papakonstantinou et P. De Hert, « The PNR agreement and Transatlantic anti-terrorism cooperation: no firm human rights framework on either side of the Atlantic », *Comm. M.L.R.*, vol. 46, n° 3, 2009, pp. 885-919 ; E. Brouwer, *Digital Borders and Real Rights*, *op. cit.* ; E. Brouwer, « Data surveillance and border control in the EU », *op. cit.* ; V. Mitsilegas, « The transformation of privacy in an era of pre-emptive surveillance », *Tilburg Law Review*, vol. 20, n° 1, 2015, pp. 35-57.

porter le regard sur les différentes formes de circulation et, donc, à « *place stronger emphasis on the multiplicity of mobilities and their intersections* »(22). Ceci veut dire, dans le cas de la directive PNR, saisir ce programme en se penchant sur la manière dont la circulation des données est organisée pour accompagner et contribuer à gérer la mobilité des voyageurs aériens.

L'approche conceptuelle de cette contribution s'inspire d'une tradition d'« études sur la gouvernementalité »(23) qui se veut attentive aux instruments gouvernementaux concernant l'élaboration d'un savoir utile à « conduire les conduites » et, donc, à constituer des « subjectivités » qui puissent être gouvernées(24). Dans ce chapitre, cela revient à explorer un programme de gouvernement spécifique (la directive PNR) qui vise à extrapoler un savoir pratique (l'identification des possibles suspects) à partir de l'aménagement d'une multitude de personnes (les passagers), de choses (les données et les infrastructures numériques) et des possibles relations (les analyses algorithmiques des données). Même si plusieurs travaux ont déjà souligné l'importance des technologies numériques pour gouverner la circulation d'une population(25), moins d'attention a été accordée aux débats concernant et façonnant le gouvernement de cet appareillage(26). Cela implique de se pencher aussi sur les manières au travers desquelles les institutions

(22) T. Basaran et E. Guild, « Mobilities, ruptures, transitions », in T. Basaran, D. Bigo, E.-P. Guittet et R.B.J. Walker (éd.), *International Political Sociology. Transversal Lines*, London, Routledge, 2017, pp. 272-285.

(23) M. Foucault, *Sécurité, territoire, population : cours au Collège de France, 1977-1978*, Paris, Seuil, 2004 ; M. Dean, *Governmentality: Power and Rule in Modern Society*, London, SAGE, 1999 ; W. Walters, *Governmentality: Critical Encounters*, New York, Routledge, 2012. Parmi les « études sur la gouvernementalité » les plus importantes se focalisant sur l'Europe, voy. B. İşleyen, « The European Union and neoliberal governmentality: twinning in Tunisia and Egypt », *European Journal of International Relations*, vol. 21, n° 3, 2015, pp. 672-90 ; M. Merlingen, « From governance to governmentality in CSDP: towards a Foucauldian research agenda », *Journal of Common Market Studies*, vol. 49, n° 1, 2011, pp. 149-169 ; W. Walters et J.H. Haahr, *Governing Europe. Discourse, Governmentality and European Integration*, Oxon, Routledge, 2005.

(24) M. Foucault, « Le sujet et le pouvoir », in M. Foucault (éd.), *Dits et écrits 1954-1988*, Paris, Gallimard, 1994, pp. 1041-1062. Voy. aussi : P. Lascoumes et P. Le Galès, « Introduction », *op. cit.*

(25) Entre autres : M.B. Salter, « To make move and let stop: mobility and the assemblage of circulation », *Mobilities*, vol. 8, n° 1, 2013, pp. 7-19 ; M.B. Salter, « Imagining numbers », *op. cit.* ; M. Leese, « The new profiling: algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union », *Security Dialogue*, vol. 45, n° 5, 2014, pp. 494-511 ; P. Pallister-Wikins, « How walls do work: security barriers as devices of interruption and data capture », *Security Dialogue*, vol. 47, n° 2, 2016, pp. 151-164.

(26) La littérature des approches critiques de la sécurité s'est principalement penchée sur le rôle de la notion de « risque ». Voy., p. ex., L. Amoore, *The Politics of Possibility. Risk and Security Beyond Probability*, Durham, Duke University Press, 2013 ; C. Aradau et R. Van Munster, « Governing terrorism through risk: taking precautions, (un)knowing the future », *European Journal of International Relations*, vol. 13, n° 1, 2007, pp. 89-115.

européennes visent à utiliser la protection de données personnelles pour « bien traduire » les individus en données en respectant l'esprit de l'ELSJ, qui se veut soucieux du respect des droits fondamentaux. Dans ce sens, la première étape de ce travail est d'offrir, dans la prochaine section, un aperçu « généalogique » de l'émergence des données PNR à la fois en tant qu'un outil potentiel de sécurité et en tant qu'un objet de débats sur comment en assurer une protection adéquate.

3. – Une brève histoire des PNR

Les PNR sont des informations sur les passagers aériens qui sont générées en format numérique lors de la réservation d'un vol. Elles sont généralement stockées dans des systèmes centralisés de réservation et principalement utilisées par les compagnies aériennes à des fins commerciales. Les systèmes informatiques qui traitent ces données ont été développés dès la fin des années 1950 et introduits vers la moitié des années 1960, pour mieux organiser la gestion d'un nombre grandissant de réservations de voyages en avion (27). Les PNR fonctionnent comme des dossiers numériques : elles contiennent des informations sur le nom du passager, l'itinéraire du voyage réservé, les méthodes de paiement utilisées et l'embarquement dans l'avion. Depuis les années 1990, plusieurs acteurs de la sécurité aux États-Unis (tels que des autorités policières ou de contrôle aux frontières) ont commencé à s'intéresser à cette source d'information afin, principalement, d'identifier des voyageurs suspects qui auraient pu être impliqués dans des trafics illégaux. À ce stade, le traitement des PNR était limité aux informations mises à disposition par les transporteurs aériens au cas par cas et généralement dans le cadre d'une coopération volontaire (28). À la suite de l'adoption de l'« *Aviation and Transportation Security Act* » en 2001 (29), le traitement des données PNR s'est généralisé et il est progressivement devenu un système opérant à grande échelle.

Aujourd'hui, les informations concernant tous les passagers d'avion en lien avec les États-Unis sont capturées et analysées par un module spécial de l'« *Automated Targeting System* », un programme high-tech

(27) M. Campbell-Kelly, *From Airline Reservations to Sonic the Hedgehog. A History of the Software Industry*, Cambridge, MA, The MIT Press, 2004, pp. 41 et s.

(28) R.U.C. Jacksta, *United States and European Union Passenger Name Record (PNR)*. PowerPoint Presentantion for the EU-US PNR Joint Review, Washington DC, Department of Homeland Security, 2005.

(29) United States of America, *Aviation and Transportation Security Act*, 49 U.S.C. 44909(C)(3).

géré par le service appel *Customs and Border Protection* (30). La création de ce système s'est accompagnée (et elle a été en partie influencée) par plusieurs débats aux niveaux national et transatlantique, concernant principalement l'introduction des techniques de profilage, leurs implications pour la vie privée et la coopération avec l'Union européenne. Une partie de ces discussions a débouché sur la conclusion d'une série d'accords bilatéraux entre le *Department of Homeland Security* et les institutions européennes. Ces mêmes accords sont cependant devenus un objet de contestation politique, de conflit interinstitutionnel et de jurisprudence au niveau européen (31). Le dernier accord, en vigueur depuis 2012, réglemente la transmission, le stockage et le traitement des données PNR « européennes » (32). En plus des États-Unis, d'autres pays ont mis en place un système de traitement des PNR à des fins de sécurité : le Canada et l'Australie ont notamment signé des accords avec l'Union européenne concernant la transmission des informations et la coopération policière (33). La proposition d'un nouvel accord avec le Canada, avancée par la Commission en 2014, a été objet, le 26 juillet 2017, d'un avis négatif de la Cour de justice de l'Union européenne, qui avait été saisie par le Parlement européen (34). La Grande Chambre de la Cour a déclaré le projet d'accord avec le Canada incompatible avec la Charte des droits fondamentaux de l'Union européenne, notamment avec les articles portant sur le respect de la vie privée (art. 7) et la protection des données personnelles (art. 8), et ceci à la suite, entre autres, d'un manque de « bonne gouvernance » liée à la gestion des données PNR (35).

(30) US DHS Privacy Office, *Privacy Impact Assessment for the Automated Targeting System*, Washington, DC, Department of Homeland Security, 2012.

(31) Voy. V. Papakonstantinou et P. De Hert, « The PNR agreement and transatlantic anti-terrorism cooperation », *op. cit.* ; F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, *op. cit.*

(32) Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la Sécurité intérieure, *JO*, L 215/5 du 11 août 2012.

(33) Accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données relatives aux informations préalables sur les voyageurs et aux dossiers passagers, *JO*, L 082/15 du 21 mars 2006, et *JO*, L 270/345 du 29 septembre 2006 ; et Accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières, *JO*, L 186/4 du 14 juillet 2012.

(34) Unité de la presse et de l'information, *Communiqué de presse n° 84/17 – Avis 1/15*, Luxembourg, Cour de justice de l'Union européenne, 2016.

(35) Avis de la Cour (gde ch.) du 26 juillet 2017, *Avis rendu en vertu de l'article 218, paragraphe 11, TFUE – Projet d'accord entre le Canada et l'Union européenne – Transfert des données des dossiers passagers aériens depuis l'Union vers le Canada – Bases juridiques appropriées – Article 16, paragraphe 2, article 82, paragraphe 1, second alinéa, sous d), et article 87, paragraphe 2, sous a), TFUE – Compatibilité avec les articles 7 et 8 ainsi qu'avec*

Au niveau européen, même si seul le Royaume-Uni possède un système en fonction (36), les initiatives politiques et législatives visant à introduire la capture et le traitement à grande échelle des PNR se sont multipliées au cours des dix dernières années. Deux propositions ont été avancées par la Commission européenne, en 2007 et 2011 (37), et les débats institutionnels ont été ensuite relancés en 2011 pour s'arrêter en 2013 lors du vote négatif au sein de la Commission LIBE (« Libertés civiles, justice et affaires intérieures ») du Parlement européen (38). Les controverses se sont concentrées à ce moment sur l'impact d'un tel système en matière de vie privée ainsi que sur le rôle de la protection des données et sur le choix des architectures informatiques nécessaires pour garantir le bon fonctionnement d'un régime de transfert et de traitement des données (39).

À la suite des attaques à Paris en janvier et novembre 2015, plusieurs acteurs institutionnels, principalement des ministres des Affaires intérieures, ont à nouveau souligné la nécessité de construire un régime UE pour les PNR (40). C'est un discours politique concernant les dangers de la circulation des individus (et, en partie, de la libre circulation dans le sens le plus classique) qui a justifié un nouvel élan sécuritaire : les données des dossiers passagers permettraient d'identifier les potentiels

l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, Avis 1/15.

(36) W.L. Allen et B.A. Vollmer, « Clean skins: making the e-border security assemblage », *Environment and Planning D: Society and Space*, 2017.

(37) Commission européenne, *Proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (*Passenger Name Record – *PNR) à des fins répressives*, COM(2007) 654 final ; Commission européenne, *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*, COM(2011) 0032 final. Voy. aussi : R. Bellanova et D. Duez, « 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, n° 2/1, 2012, pp. 109-124 ; F. Boehm, « EU PNR: European flight passengers under general suspicion - The envisaged European model of analyzing flight passenger data », in S. Gutwirth, Y. Poullet, P. De Hert et R. Leenes (éd.), *Computers, Privacy and Data Protection: An Element of Choice*, Dordrecht, Springer, 2011, pp. 171-199 ; P. De Hert et V. Papakonstantinou, « The EU PNR framework decision proposal: towards completion of the PNR processing scene in Europe », *Computer Law & Security Review*, vol. 26, n° 4, 2010, pp. 368-376.

(38) European Parliament Press Unit, *Civil Liberties Committee rejects EU Passenger Name Record proposal, [Press release]* disponible sur http://www.europarl.europa.eu/news/en/news-room/content/20130422IPR07523/Civil-Liberties-Committee-rejects-EU-Passenger-Name-Record-proposal, consulté le 10 janvier 2018.

(39) R. Bellanova et D. Duez, « A different view on the "making" of European security », *op. cit.* Voy. aussi : N. Huijboom et G. Bodea, « Understanding the political PNR-debate in Europe: a discourse analytical perspective », *Perspectives on European Politics and Society*, vol. 16, n° 2, 2015, pp. 241-255.

(40) N. Nielsen, « EU ministers back air passenger data sweep », *EUobserver.com*, 4 décembre 2015, disponible sur https://euobserver.com/justice/131395.

« *returning jihadists* » ou « *foreign fighters* » voyageant entre l'Europe et le Moyen-Orient. Ainsi, la proposition d'un système paneuropéen pour la capture et le traitement des PNR est devenue une priorité stratégique pour la lutte contre le terrorisme (41). Cette fois, la Commission LIBE a donné son feu vert au texte législatif négocié en 2015, tout en insistant à la fois sur les sauvegardes nécessaires pour la protection des données personnelles et sur l'importance majeure de la mesure pour assurer la sécurité européenne (42). Avec le soutien du Parlement européen, les principales résistances institutionnelles à l'introduction d'un programme de gouvernement axé sur la collection massive et le traitement des données des dossiers passagers sont tombées : la directive PNR a été ainsi finalement adoptée en avril 2016 après plus de dix ans de controverses.

Le lancement de ce projet ne se fait pas pour autant sans poser de problème. Le Contrôleur européen de la protection des données (l'institution européenne se focalisant sur la protection de données personnelles) a, par exemple, réaffirmé sa critique à l'égard de la rationalité sous-tendant ce programme : la législation introduit un système de surveillance de masse en Europe (43). De plus, la mise en place du système s'annonce déjà difficile et lente. Nonobstant l'urgence qui avait caractérisé son approbation lors des dernières négociations institutionnelles, seul un nombre limité de pays européens a lancé concrètement les démarches nécessaires à sa mise en œuvre du point de vue institutionnel, législatif ou technique (44). En d'autres mots, la directive PNR risque de ne pas échapper aux trappes de la transposition juridique et de l'implémentation opérationnelle qui sont désormais si typiques de l'ELSJ (45).

En somme, les PNR sont des données qui naissent pour gérer la circulation des voyageurs : elles sont la solution au problème posé par la croissance de la mobilité par voie aérienne. Depuis plusieurs décennies, les systèmes commerciaux traitant les PNR ont créé une forme de circulation qui accompagne, ou, mieux, précède et façonne,

(41) Voy. Commission européenne, *Le programme européen en matière de sécurité*, *op. cit.*

(42) European Parliament Press Service, *EU Passenger Name Record (PNR): Civil Liberties Committee backs EP/Council deal*, Bruxelles, 2015.

(43) European Data Protection Supervisor (EDPS), *EU PNR: EDPS Warns against Unjustified and Massive Collection of Passenger Data [Press release]*, Bruxelles, 2015.

(44) Commission européenne, *Commission Staff Working Document: Implementation Plan for Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, Bruxelles, 2016.

(45) S. Lavenex, « Justice and home affairs », *op. cit.*, pp. 385-386.

la circulation des individus et des avions les transportant. Plusieurs acteurs de la sécurité, et certainement un acteur majeur tel que la Commission européenne, se sont intéressés aux PNR en tant que source d'information précieuse qui permettrait de contrôler discrètement les passagers et d'identifier des suspects encore inconnus des autorités. Si, désormais, la plupart des acteurs européens paraissent avoir accepté l'idée que la circulation des voyageurs doit être surveillée, la question de la manière d'organiser la mobilité des données de dossiers passagers paraît se démultiplier. Cette double ambition gouvernementale, *mieux* gouverner par les données et *bien* gouverner les données, est au cœur de la directive PNR.

4. – La double ambition gouvernementale projetée par la directive PNR

L'usage des techniques pour collecter et classer des informations, et donc gouverner une population, est une « technologie politique » qui accompagne et caractérise la modernité européenne (sans lui être exclusive) depuis plusieurs siècles (46). En ce qui concerne la gestion de la sécurité, on identifie au moins deux archétypes de cette technologie politique. D'un côté, certaines formes de surveillance fonctionnent en « arrêtant » les individus et en les traduisant en données qui sont stockées pour faciliter l'identification de chaque personne. Cette rationalité est, par exemple, au cœur des pratiques de numérisation aux frontières, où les « *walls* do *work* » parce que « *they interrupt circulation and facilitate data capture* » (47). D'un autre côté, des systèmes s'appuient sur les informations engendrées par les mouvements des individus. Étant donné que les personnes peuvent et parfois doivent bouger, elles produisent des traces qui, moyennant les ressources et les infrastructures nécessaires, peuvent être collectées et ensuite être utilisées pour l'aménagement de ces flux. Cette rationalité sous-tend le régime

(46) T. Berns, *Gouverner sans gouverner. Une archéologie politique de la statistique*, Paris, Presses universitaires de France, 2009 ; A. Desrosières, « Le gouvernement de la cité néolibérale : quand la quantification rétroagit sur les acteurs », in A. Desrosières (éd.), *Prouver et gouverner. Une analyse politique des statistiques publiques*, Paris, La Découverte, 2014, pp. 33-59 ; M. Foucault, *Sécurité, territoire, population*, *op. cit.* ; N. Rose, *Powers of Freedom. Reframing Political Thought*, Cambrindge, Cambridge University Press, 1999. Le lien entre la collection des informations et la possibilité d'exercer une forme de contrôle sur les individus est établi de manière explicite dans la définition de surveillance proposée par Lyon : « [surveillance] *is the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction* », D. Lyon, *Surveillance Studies. An Overview*, Cambridge, Polity, 2007, p. 14.

(47) P. Pallister-Wikins, « How walls do work », p. 152, en italique dans l'original.

européen concernant les PNR (48) : les informations ne sont pas introduites par les autorités après avoir arrêté les individus, elles sont plutôt capturées à partir des traces engendrées par les voyageurs eux-mêmes. Entre ces deux archétypes de technologies de sécurité, il y a toute une panoplie de pratiques qui fonctionnent en combinant en quelque sorte les deux rationalités. Par exemple, à travers le SIS, les autorités de police d'un pays Schengen peuvent, dans certains cas, essayer de plus en connaître à propos d'un potentiel suspect sans devoir l'« arrêter » parce qu'elles ont accès aux données collectées et stockées par les autorités d'un autre État Schengen.

La directive PNR intervient dans la circulation des données des dossiers passagers en obligeant les compagnies aériennes à transférer une copie de ces informations (49) aux « unités d'information passagers » (UIP), des autorités nationales spécialement conçues pour traiter ces informations et détecter des suspects (50). Dès que la législation sera transposée et appliquée, les informations concernant tous les passagers voyageant sur des « vols extra-UE », c'est-à-dire entre l'Union européenne et un pays tiers, seront capturées, stockées et traitées par les UIP. En se greffant à l'architecture numérique déjà existante, qui permet notamment d'engendrer et d'organiser les données qui seront finalement transmises aux UIP, le régime européen vient créer une nouvelle forme de circulation des données à partir du milieu commercial. Ainsi, la première dynamique gouvernementale que l'on identifie dans la directive PNR concerne le processus de numérisation. Au lieu de « *datify* » *ex novo* chaque voyageur, c'est-à-dire de « *put* [*a phenomenon*] *in a quantified format so it can be tabulated and analyzed* » (51), le régime PNR opère à partir d'une masse de données numériques qui lui sont fournies parce qu'elles sont déjà numérisées par les systèmes commerciaux des compagnies aériennes. Les systèmes

(48) Voy. l'analyse du projet européen PNR faite par M. Leese (« The new profiling », *op. cit.*), qui souligne les affinités entre le système de profilage à travers les données passagers et le fonctionnement des « dispositifs de sécurité » tels que conceptualisés par Foucault (*Sécurité, territoire, population*, *op. cit.*).

(49) L'article 1(1)(a) de la directive PNR mentionne que « [l]a présente directive prévoit : (a) le transfert, par les transporteurs aériens, de données des dossiers des passagers (PNR) de vols extra-UE ».

(50) Voy. l'article 4 de la directive PNR établissant la « désignation » par les États membres d'« une autorité compétente en matière de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière […] en tant que son UIP ».

(51) V. Mayer-Schönberger et K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Boston, Eamon Dolan, 2013, p. 78.

de réservation utilisés par les compagnies aériennes, et *a fortiori* par les voyageurs, sont donc les capteurs numériques principaux.

La gestion de la circulation d'une masse de données, plutôt que le contrôle de la mobilité des voyageurs, est l'objectif « préalable » du système de sécurité PNR. En effet, même si cette circulation est déjà en format numérique, cette masse de données doit encore être ordonnée et traitée. La directive PNR vise à organiser cette nouvelle forme de circulation de plusieurs manières : elle identifie quelles informations doivent être envoyées parmi celles qui ont été collectées au moment de la réservation (52) et elle définit les modes de transmission des informations entre les transporteurs aériens et les UIP. Ainsi, les données PNR doivent être envoyées en utilisant un système dit « push », à travers lequel les compagnies aériennes doivent « activement » transférer les informations au moins à deux reprises avant le départ de l'avion (53). Ces acteurs commerciaux devront adopter des « protocoles communs » et des « formats de données reconnus » tels qu'ils seront définis par la Commission européenne (54). Le processus de numérisation des voyageurs ne s'arrête pas à la simple capture des données PNR par les UIP. La directive PNR se penche aussi sur l'organisation des données une fois qu'elles ont été reçues par les UIP, en explicitant comment et pour combien de temps elles doivent être stockées, y compris leur « dépersonnalisation » (55), et surtout comment elles peuvent être traitées à des fins de sécurité (56).

Le projet de système européen PNR a déjà été l'objet d'études, notamment à la suite de l'introduction des technologies de sécurité opérant à partir d'algorithmes de profilage (57). En effet, parmi les traitements légitimes des données, la directive PNR reconnaît la possibilité de : « a) réaliser une évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci » (58). Cette « évaluation » peut se faire soit à partir une comparaison avec des bases de données ou des requêtes ponctuelles de la part d'autorités compétentes, soit à travers leur traitement « au regard de critères préétablis » (59). Ainsi, les données PNR peuvent être utilisées à la fois pour le travail

(52) Annexe I de la directive PNR.
(53) Art. 8 de la directive PNR.
(54) Art. 16 de la directive PNR.
(55) Art. 12 de la directive PNR.
(56) Art. 6 de la directive PNR.
(57) R. Bellanova et D. Duez, « A different view on the "making" of European security », *op. cit.* ; M. Leese, « The new profiling », *op. cit.*
(58) Art. 6(2)(a) de la directive PNR.
(59) Art. 6(3) de la directive PNR.

d'enquête plus traditionnel et pour une surveillance préventive et généralisée des passagers. Dans les deux cas, la « circulation continue » des données des dossiers passagers offre aux UIP un avantage par rapport à la « liberté de mouvement » des individus et leur permet de la gouverner « à distance ».

Ce qui reste moins étudié est que l'introduction de cet « imaginaire cybernétique » par la directive PNR repose sur une deuxième ambition gouvernementale : celle de protéger les données personnelles. En effet, l'aménagement de la circulation des PNR décrite plus haut ainsi que de toute une série d'autres pratiques touchant à l'organisation même des UIP, est principalement animé par un souci de protéger les PNR en tant que données personnelles. Dans le cadre de l'Union européenne, toute donnée personnelle, c'est-à-dire « toute information se rapportant à une personne physique identifiée ou identifiable », (60) est l'objet d'une législation visant à protéger les personnes auxquelles la donnée fait référence (61). Cette législation vient également clarifier les conditions auxquelles la circulation des données elles-mêmes peut avoir lieu. En d'autres mots, la législation qui porte sur les données personnelles protège les personnes en leur conférant une série de droits par rapport au traitement de leurs données et en intervenant directement sur les manières dont on peut les faire circuler.

Le double objectif stratégique de la protection des données personnelles – protection et circulation – engendre une sorte d'ambiguïté concernant ses possibles mobilisations (62). Elle peut, d'une part, devenir un outil pour les individus en tant que droit fondamental et offrir ainsi une manière d'intervenir dans les pratiques de gouvernement des acteurs qui collectent et traitent leurs données (63). D'autre part, elle peut être mobilisée par ceux qui gouvernent et qui veulent organiser la circulation de données. Étant donné que les PNR sont conceptualisées comme des données personnelles par tous les acteurs concernés, la protection de données personnelles est mobilisée par les

(60) Art. 3(1) de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *JO*, L 119/89, du 4 mai 2016.

(61) L.A. Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits*, The Hague, Kluwer Law International, 2002.

(62) R. Bellanova, « Digital, politics, and algorithms: governing digital data through the lens of data protection », *European Journal of Social Theory*, vol. 20, n° 3, 2017, pp. 329-347.

(63) C. Norris, P. De Hert, X. L'Hoiry et A. Galetta (éd.), *The Unaccountable State of Surveillance. Exercising Access Rights in Europe*, Dordrecht, Springer, 2017.

institutions européennes pour informer et justifier l'aménagement de la circulation des PNR. En d'autres mots, la protection des données personnelles devient ici un outil cognitif utile pour appréhender les données en tant que problème gouvernemental et pour essayer de le résoudre. Elle est utilisée afin d'en tirer des lignes de conduite utiles à assurer une « bonne traduction » de voyageurs en PNR. Tout en identifiant des limites à la collection, l'échange, le stockage et le traitement des données de dossiers passagers, la directive PNR crée les conditions nécessaires à gouverner les données et ainsi les passagers. Elle présente, par exemple, les formes de traitement comme des « exceptions » à une règle plus générale de non-traitement (64), tout en introduisant, finalement, un système de surveillance numérique à grande échelle.

Cette double ambition gouvernementale – numérisation des passagers et protection des PNR – produit de nouvelles « subjectivités » qui concernent non seulement les individus, mais aussi les données (65). D'abord, on voit les deux « prises » sur les voyageurs à travers les données PNR, et, donc, les deux pratiques de « subjectivation » mises en place pour gouverner la circulation des individus. Dans le premier cas, le traitement vise à identifier un individu qui est déjà connu, qui a déjà été « subjectivé » au préalable comme suspect, soit parce que ses données personnelles sont déjà stockées dans une banque d'informations, soit parce qu'une autorité l'a signalé à une UIP. Dans le deuxième cas, les profils de possibles suspects se construisent aussi à travers le traitement « en masse » des données PNR déjà stockées, afin d'aider les analystes à détecter des corrélations, des liens et des tendances qui émergeraient de situations similaires. Ici, la « subjectivation » du passager en tant que potentiel suspect repose avant tout sur l'analyse d'une population, qui est, cette fois, principalement constituée de données. Le gouvernement de la mobilité humaine à travers la circulation des PNR engendre trois formes supplémentaires de « subjectivation », certes plus faibles, mais pas de moindre importance pour le fonctionnement du système européen PNR dans le cadre de l'ELSJ. D'abord, il y a la production des voyageurs non suspects, ceux qui ne seront pas signalés pour des contrôles supplémentaires, et qui, en principe, circulent donc sans entraves et témoignent du « bon » fonctionnement d'une circulation finalement « libre ». Une deuxième forme de

(64) Art. 6(2) de la directive PNR.

(65) Sur la « protection » en tant qu'ambition gouvernementale, voy. D. Bigo, « Protection. Security, territory and population », in J. Huysmans, A. Dobson et R. Prokhovnik (éd.), *The Politics of Protection. Sites of Insecurity and Political Agency*, London, Routledge, 2006, pp. 84-100.

« subjectivation » concerne toute PNR stockée dans les banques des UIP, surtout après sa « dépersonnalisation », ou échangée avec d'autres autorités. Ceci sera « traitée » en tant que partie d'une population numérique qui pourrait contribuer, à un certain moment, à la production d'un savoir. *In fine*, tous les passagers – suspects ou pas – seront à considérer comme des sujets numériques (« *data subjects* »), ayant des droits bien définis vis-à-vis du système PNR, par exemple l'accès à ses propres données et à la rectification de ces informations au cas où elles seraient erronées (66). Pour autant, ces sujets numériques n'ont pas la possibilité de sortir du système, sauf en décidant de ne plus réserver de vol extra-UE et, donc, d'organiser leur mobilité à travers d'autres moyens de transport.

En somme, le régime de surveillance des passagers présuppose que les données PNR circulent et il requiert l'organisation d'un dispositif qui puisse réguler la mobilité de ces données. À présent, la directive PNR reste principalement un dispositif juridique, car il introduit les conditions qui facilitent la création d'un cadre législatif dans chaque État membre de l'Union européenne. Mais ce dispositif fonctionne aussi comme « marqueur » des choix techniques, par exemple, concernant les types d'information à transférer aux UIP, et des choix politiques, par exemple la décision de traiter et de stocker les données PNR de tous les voyageurs sur les vols extra-UE, que ces individus soient ou non citoyens européens. En effet, c'est seulement une fois que les données sont transférées aux autorités nationales qu'elles font partie d'un système informatique avancé où elles peuvent être légitimement et légalement traitées et échangées « à des fins de prévention et de détection des infractions terroristes et des formes graves de criminalité[,] ainsi que d'enquête et de poursuites en la matière » (67). C'est principalement grâce à la mise en place d'un cadre qui prend en compte la protection des données personnelles que le choix politique d'introduire un système de surveillance de masse de cette envergure peut s'opérer au niveau européen. La protection des données personnelles n'opère pas dans ce cas principalement en tant que droit fondamental, mais elle est transformée en un dispositif politico-technique qui permet de gouverner les données, les systèmes informatiques qui doivent les traiter, et même les acteurs qui opèrent ces technologies (les UIP). Pour reprendre les mots de Foucault : « il ne s'agit pas d'imposer une loi aux hommes, il s'agit de disposer des choses, c'est-à-dire d'utiliser plutôt des tactiques que

(66) Art. 13 de la directive PNR.
(67) Art. 1(2) de la directive PNR.

des lois, ou d'utiliser au maximum des lois comme des tactiques ; faire en sorte, par un certain nombre de moyens, que telle ou telle fin puisse être atteinte » (68).

En faisant de la protection des données l'un des deux objectifs explicites de la directive PNR, les institutions européennes ont essayé de « disposer les choses » en utilisant cette législation de manière « tactique », c'est-à-dire qu'elles aménagent un milieu qui permet de gouverner les données, les techniques d'analyse, les nouvelles autorités (UIP) et, par conséquent, les passagers. La directive PNR vient ainsi modifier l'environnement de la sécurité européenne. « Traduire » les voyageurs aériens dans « leurs » données des dossiers passagers ouvre à de nouvelles techniques gouvernementales, comme le profilage et la surveillance de masse. Toutefois, ce processus de numérisation charge aussi les acteurs de la sécurité avec la tâche de « bien » gouverner une multitude de nouveaux sujets, tant humains (les passagers) que non humains (leurs données PNR).

5. – Conclusions

Ce chapitre a brièvement retracé l'entrée en jeu des données des dossiers passagers dans les projets de gestion de la mobilité humaine et de construction de l'ELSJ. Il a ensuite proposé une esquisse analytique d'une double dynamique liée à la gouvernance de la libre circulation à travers la circulation des PNR. D'un côté, la directive PNR souligne comment l'accès aux données commerciales est de plus en plus considéré par les acteurs de la sécurité européenne comme une source d'information précieuse pour pouvoir contrôler les mouvements des personnes. De l'autre côté, le texte de la directive PNR montre comment ces mêmes acteurs doivent aussi s'investir dans le gouvernement des données numériques. Ils doivent assurer les conditions techniques nécessaires à la mise en place d'une circulation des données et ils sont tenus à appliquer les lois relatives à la protection des données personnelles.

Ce qui apparaît est donc une sorte de « gouvernementalité numérique européenne » : on observe à la fois un effort d'ordonner (dans le double sens de classer et d'imposer un ordre) à travers les données personnelles *et* une réflexion sur les manières de protéger et ainsi de gouverner les données en tant que telles. En d'autres mots, cette contribution montre

(68) M. Foucault, *Sécurité, territoire, population*, *op. cit.*, p. 103.

que le processus de numérisation de la libre circulation *et* de sa régulation conçoit les données non seulement comme un instrument pour « mieux » gouverner, mais aussi comme un objet qui doit être « bien » gouverné. Ce mode de gouvernement ne s'opère pas dans le vide, mais nécessite un environnement institutionnel, juridique et technique pour fonctionner en adéquation avec les ambitions de l'ELSJ, en lien en particulier avec la rationalité de la protection de données personnelles qui implique d'assurer la circulation des données et le respect des droits fondamentaux. Une lecture de la gouvernementalité « projetée » par la directive PNR nous permet de saisir la construction de l'ELSJ dans une dimension plus matérielle, mais qui n'est pas pour autant moins politique.

Cette manière de problématiser la construction de l'ELSJ permet aussi d'élargir la manière d'envisager la question de la libre circulation qui est au cœur de cet ouvrage. Depuis une perspective plus « classique », la gestion de la libre circulation permet de saisir les dynamiques de l'intégration européenne dans un champ touchant directement aux pouvoirs régaliens de l'État, et ainsi d'étudier de plus près l'institutionnalisation de l'ELSJ entre intergouvernementalisme et communautarisation (69). Depuis une perspective plus « critique », la gestion de la libre circulation peut être étudiée comme un cas qui met au jour les tensions au cœur de la construction de l'ELSJ, où sécurité, justice et liberté sont à la fois démultipliées et parfois jouées les unes contre les autres (70). *In fine*, les études de la gouvernementalité nous permettent de saisir la gestion de la libre circulation non seulement comme un élément clé dans la construction d'un nouvel espace d'intervention politique, mais aussi comme la constitution d'une population à gouverner à travers des technologies qui, à leur tour, contribuent à une nouvelle « subjectivation » de ceux qui sont supposés circuler librement (71). Ce chapitre contribue à cette dernière approche en soulignant comment les pratiques de numérisation transforment les individus tout en participant aussi à constituer une nouvelle population faite par les données, une population quasi à part entière, et qui va donc (devoir) être à son tour gouvernée et problématisée en tant que telle. Les manières dont ce problème est *et* sera « résolu » dans la pratique des acteurs sont des enjeux éminemment politiques, et ils sont ainsi à étudier de la sorte.

(69) F. Trauner et A. Ripoll Servent (éd.), *Policy Change in the Area of Freedom, Security and Justice. How EU Institutions Matter*, London, Routledge, 2015.

(70) D. Bigo, « Un espace de liberté, de sécurité et de justice ? », *op. cit.*

(71) W. Walters et J. H. Haahr, *Governing Europe*, *op. cit.*