L'utilisation de la biométrie et des RFIDs dans le cadre de l'espace européen de liberté, de sécurité et de justice

Dumortier, Franck

Published in:
ERA Forum

Publication date:
2009

Document Version
le PDF de l'éditeur

ERA Forum (2009) 9: 543–579
DOI 10.1007/s12027-008-0094-z

ARTICLE

L'utilisation de la biométrie et des RFIDs dans le cadre de l'espace européen de liberté, de sécurité et de justice : une affaire de balance ou une question de dignité ?

Using biometrics and RFIDS chips in the European Area of Liberty, Security and Justice—a question of balance or a question of dignity?

Franck Dumortier

Published online: 10 February 2009

Résumé Dans la présente contribution, l'auteur rappelle que les droits de l'Homme constituent la limite principale et le fondement de l'association politique et que ceux-ci découlent d'une caractéristique essentielle de l'être humain : sa dignité. Après avoir rappelé le sens de ce concept fondateur, l'auteur examine ses implications sur l'interprétation du droit au respect de la vie privée au regard de l'utilisation de RFIDs et de la biométrie au sein de l'espace JLS. Au vu de l'importance des risques de dérive, l'auteur argue que le droit au respect de la vie privée ne peut en aucun cas être mis en « balance » avec un prétendu droit à la sécurité. Afin de respecter la limite et la raison d'être du Pouvoir, les ingérences de l'autorité publique doivent respecter la dignité humaine et rester strictement nécessaires dans une société démocratique.

Mots-clefs Droits de l'Homme · Immigration · Contrôle aux frontières · Protection des données à caractère personnel · Principe de précaution

Abstract This article discusses the problems attached to the storage of personal data relating to identity documents and residence permits in automated data storage systems. It highlights how these problems are exacerbated by the use of biometric elements and RFID. In combination with automated procedures at border crossing points

Franck Dumortier est assistant et chercheur sénior au Centre de recherches informatique et droit (CRID) des Facultés universitaires Notre Dame de la Paix (FUNDP) à Namur. L'auteur remercie Denis Darquennes pour avoir participé à l'exposé oral présenté conjointement le 26 mai 2008 à la conférence de l'ERA intitulée « Data exchange and data protection in the area of freedom, security and justice » dont la présente contribution constitue un prolongement. L'auteur remercie également chaleureusement Antoinette Rouvroy pour sa relecture attentive et ses réflexions extrêmement pertinentes ainsi que Virginie Fossoul pour ses précieux commentaires.

F. Dumortier (✉)
Université de Namur - FUNDP, 61 rue de Bruxelles, 5000 Namur, Belgique
e-mail: Franck.dumortier@fundp.ac.be

travellers may see there travel interrupted based on wrong information contained in the data storage system which they will not easily be able to correct due to the confidence put in the systems. The article puts these problems in a wider context of identity and human dignity. It reminds the reader that there is a risk of confusing immigration and criminality under the wider heading of "security". Based on a profound human rights analysis, the author takes the view that one should not easily believe that there is a mere balance to be struck between the right to protection of data of an individual concerned and the right to security of other potential crime victims or the public in general. Rather one should remember that all human rights texts are based on the idea that limitations to individual rights need to be justified by legitimate aim and in a way that is necessary in a democratic society. Finally it calls for a coherent approach by the European policy-maker relating to the collection and storage of personal data with implications for the right of persons to free movement.

Keywords Human rights · Immigration · Border controls · Protection of personal data · Precautionary principle

They that can give up essential liberty
to obtain temporary safety deserve
neither liberty nor safety.
(Benjamin Franklin's Historical Review of Pennsylvania of 1759)

1 Introduction

Depuis la signature du Traité d'Amsterdam, un des objectifs fondamentaux de l'Union européenne est d'offrir à ses citoyens un espace de *« liberté, de sécurité et de justice »* [1] (ci-après « espace JLS ») sans frontières intérieures. L'« espace normatif » qui en découle couvre, d'une part, des matières relevant du régime communautaire (1er pilier)—à savoir les politiques relatives aux contrôles aux frontières, à l'asile et à l'immigration, ainsi que la coopération judiciaire en matière civile—et, d'autre part, des matières relevant du régime intergouvernemental (3ème pilier) comme la coopération judiciaire et policière en matière pénale.[2]

Dans ce contexte, cinq ans après avoir adopté un premier programme de travail à Tampere afin d'atteindre ses objectifs, le Conseil en a lancé un second, en 2004 à La Haye, dont la mise en œuvre s'étale jusqu'en 2010. Ce dernier y rappelle que

[1] Le traité de Lisbonne signé en 2007 et soumis actuellement à ratification dans les Etats membres le rappelle dans son article 2.2 selon lequel l'« L'Union offre à ses citoyens un espace de liberté, de sécurité et de justice 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] Rappelons que depuis le Traité de Maastricht, l'Union européenne repose sur trois piliers : les Communautés européennes (1er pilier), la Politique étrangère et de sécurité commune (2ème pilier) et la coopération policière et judiciaire en matière pénale (3ème pilier). Ces piliers se distinguent avant tout par le mode de décision employé mais également par la compétence de contrôle de la C.JC.E. Ainsi, dans le 1er pilier, la procédure de décision est de type « communautaire » et implique l'ensemble des institutions. Par contre, dans les deuxième et troisième piliers, elle est de type « intergouvernemental », et le rôle du Parlement est nettement plus effacé. La compétence de la C.J.C.E. est également plus limitée dans le cadre du 3ème pilier que dans le cadre du premier.

> la question de la sécurité de l'Union européenne et de ses États membres se pose avec une acuité renouvelée, au vu notamment des attentats terroristes perpétrés aux États-Unis le 11 septembre 2001 et à Madrid le 11 mars 2004. Les citoyens d'Europe attendent à juste titre de l'Union européenne que, tout en garantissant le respect des libertés et des droits fondamentaux, elle adopte une approche commune plus efficace des problèmes transfrontières tels que l'immigration illégale, la traite des êtres humains, le terrorisme et la criminalité organisée, ainsi que de leur prévention.[3]

Afin de concrétiser ces ambitions « sécuritaires » inter-piliers allant de la lutte contre le terrorisme à la prévention et la répression de l'immigration illégale, le programme de La Haye prône avec insistance une approche innovante de l'échange transfrontière d'informations en matière répressive selon le principe de disponibilité,[4] le renforcement du recours à Europol et Eurojust, l'utilisation des données des passagers pour des impératifs de sécurité des frontières et de l'aviation et d'autres fins répressives, l'interopérabilité entre le Système d'information Schengen (SIS II), le Système d'information sur les visas (VIS) et EURODAC,[5] ainsi que l'intégration « sans tarder, des identificateurs biométriques dans les documents de voyage, les visas, les permis de séjour, les passeports des citoyens de l'UE et les systèmes d'information ».[6]

Depuis lors, les vœux du Conseil sont loin d'être restés lettre morte. Outre la multiplication des bases de données européennes contenant des éléments biométriques,[7] des efforts importants ont été menés en matière d'interopérabilité,[8] d'inter-

[3]Programme de La Haye, p. 3, disponible à l'adresse http://ec.europa.eu/justice_home/doc_centre/doc/hague_programme_fr.pdf.

[4]Conformément au programme de La Haye, ce principe signifie que « dans l'ensemble de l'Union, tout agent des services répressifs d'un État membre qui a besoin de certaines informations dans l'exercice de ses fonctions peut les obtenir d'un autre État membre, l'administration répressive de l'autre État membre qui détient ces informations les mettant à sa disposition aux fins indiquées [. . .] ». Il est par ailleurs souligné dans le programme que « les méthodes utilisées pour échanger les informations devraient exploiter pleinement les nouvelles technologies et être adaptées à chaque type d'information, s'il y a lieu, par le biais d'un accès réciproque aux banques de données nationales, de leur interopérabilité ou de l'accès direct (en ligne) ».

[5]EURODAC est un système de comparaison des empreintes digitales des demandeurs d'asile et des immigrants clandestins afin de faciliter l'application du Règlement Dublin II qui permet de déterminer l'État responsable de l'examen d'une demande d'asile. EURODAC est formé d'une unité centrale située à la Commission qui est équipée d'une base de données centrale complètement automatisée et informatisée, destinée à la comparaison des empreintes digitales, et d'un système de transmission électronique des données reliant chaque État participant à l'unité centrale. EURODAC a été mis en place par le Règlement nº 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système EURODAC pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin.

[6]Programme de La Haye, p. 4.

[7]Les bases de données SIS II et VIS contiennent des photographies et des empreintes digitales et EURODAC contient des empreintes digitales. Une nouvelle proposition concerne la collecte d'empreintes digitales dans le cadre d'un système d'entrée/sortie applicable à tous les ressortissants de pays tiers (y compris ceux qui ne sont pas soumis à visa lors de leur première entrée sur le territoire). Voy. la Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, *« Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne »* , COM (2008) 69 final, 13 février 2008. Une autre proposition concerne la création d'un système européen

connexion[9]—voire de centralisation—de celles-ci, la Commission européenne dévoilant, par exemple, que l'une de ses actions-clés pour 2008 consiste en l'établissement d'une « banque » d'empreintes digitales centralisée.[10] Dans un même mouvement, on constate une importante inflation législative dans le domaine de l'échange d'informations,[11] appliquant notamment le principe de disponibilité au transfert automatisé des profils ADN et des empreintes digitales.[12] Par ailleurs, force est de constater l'intégration progressive de plus de moyens biométriques d'identification, non seulement dans les visas et les titres de séjour délivrés aux ressortissants de pays tiers[13] mais également dans les passeports et documents de voyage délivrés par les États membres.[14] Enfin, fait non-négligeable, ces documents d'identification sont de plus

automatisé d'identification criminelle par les empreintes digitales (AFIS) dans lequel seraient rassemblées toutes les données relatives aux empreintes digitales qui ne sont actuellement disponibles que dans les AFIS nationaux. Enfin, une dernière proposition concerne la mise en place d'un « Registre européen des documents de voyage et des cartes d'identité » dans lequel les Etats membres *« introduiront aussi les données biométriques enrôlées lors de la demande »*. Voy. la Communication de la Commission européenne, du 24 novembre 2005, sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases, COM (2005) 597 final—non publiée au Journal officiel.

[8] Voy. par exemple, la Communication de la Commission européenne, du 24 novembre 2005, sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases, *op cit.* ; et la Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », *op cit*.

[9] Voy. notamment la proposition visant à créer un système européen d'information sur les casiers judiciaires (ECRIS) en vue de compléter la future Décision-cadre relative à l'organisation et au contenu des échanges d'informations extraites du casier judiciaire entre les États membres, COM (2008)0332.

[10] Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des régions du 21 février 2007, Stratégie politique annuelle pour 2008, COM (2007) 65 final.

[11] Voy. par exemple, la Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, la proposition de Décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité ; le Traité de Prüm, signé par sept États membres (Allemagne, Autriche, Belgique, Espagne, France, Luxembourg et Pays-Bas), Journal officiel C 71/35 du 28.03.2007 ; les Décisions 2008/615/JAI, 2008/616/JAI et 2008/617/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (intégrant le Traité de Prüm dans l'ordre juridique de l'UE). Voy. également la proposition de Décision-cadre du Conseil relative à l'organisation et au contenu des échanges d'informations extraites du casier judiciaire entre les Etats membres, COM (2005) 690 final.

[12] Voy. par exemple les articles 2 à 9 de la Décision 2008/615/JAI, *op cit*.

[13] Règlement (CE) n° 1030/2002 du Conseil, du 13 juin 2002, établissant un modèle uniforme de permis de séjour pour les ressortissants de pays tiers ; Proposition de Règlement du Conseil modifiant le Règlement (CE) n° 1030/2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers, COM (2003) 0558—non publié au Journal officiel.

[14] Règlement (CE) n°2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres ; Décision de la Commission du 28 juin 2006 établissant les spécifications techniques afférentes aux normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, COM (2006) 2909 final, non publié au Journal officiel. Depuis août 2006, les États membres délivrent des passeports biométriques

en plus souvent équipés de technologie RFID[15] afin de faciliter leur lecture à distance.

Ces nouveaux moyens technologiques mis à disposition des politiques européennes relevant du volet « sécuritaire » de l'espace JLS traduisent la convergence de plusieurs phénomènes *a priori* hétérogènes les uns aux autres mais se renforçant mutuellement : le surgissement d'un nouveau « paradigme sécuritaire » mêlant les objectifs précédemment indépendants de la lutte contre le terrorisme et la criminalité et de la lutte contre l'immigration illégale,[16] la collecte généralisée d'éléments biométriques dans un but d'identification[17] et d'authentification[18] « fiable » des individus, la transmission de ces éléments par radio fréquence (RFID)[19] aux autorités jugées compétentes, l'interopérabilité des bases de données en vue de leur interconnexion et enfin un échange accru d'informations rendu possible grâce au principe de disponibilité. L'ensemble de ces caractéristiques préfigure un espace de justice, de liberté et de sécurité basé sur une large dissémination de « capteurs » (RFIDs et biométriques)

contenant l'image faciale numérisée du titulaire ; à partir du 28 juin 2009, les passeports contiendront également les empreintes digitales.

[15]En vertu de la Décision de la Commission du 28 juin 2006, précitée, les Etats Membres sont tenus d'utiliser des puces RF (à radio fréquences) comme support de stockage dans leurs documents de voyage et leurs passeports.

[16]A cet égard, le Conseil « Justice et affaires intérieures » qui s'est réuni à Luxembourg les 12 et 13 juin 2007 illustre bien cette confusion des objectifs entre criminalité, terrorisme et immigration. A cette occasion, le Conseil a en effet a invité la Commission à présenter dans les plus brefs délais une modification du Règlement EURODAC afin de permettre aux services de police et aux services répressifs des États membres ainsi qu'à Europol d'avoir accès, dans certaines conditions, à EURODAC, base de données conçue initialement comme instrument pour l'application du Règlement de Dublin.

[17]L'identification permet de connaître une identité d'une entité, c'est-à-dire de déterminer l'identité d'un individu au sein d'une certaine population, elle nécessite une « one-to-many comparison » afin d'identifier l'utilisateur parmi l'ensemble des personnes enregistrées. Voy. la définition proposée à l'ISO : *« Recognizing an entity within some context with unique identity references and additional information that characterizes the entity »* (http://www.jtc1sc27.din.de/sce/SD6).

[18]L'authentification est un processus qui consiste à vérifier l'identité prétendue d'une personne donnée afin d'obtenir l'assurance que l'individu est bien la personne qu'il prétend être, elle ne nécessite qu'une « one-to-one comparison », une comparaison des données transmise avec l'information préalablement enrôlée appartenant à une seule personne. Voy. la définition de l'ISO : « Provision of assurance of the claimed identity of an entity. In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication) » (ISO/IEC 18028-4 : 2005).

[19]Dans son projet de Recommandation sur la mise en œuvre des principes relatifs à la vie privée, la protection des données et la sécurité de l'information dans les applications soutenues par la RFID de février 2008, la Commission définit l'identification par radio fréquence (RFID) comme « l'utilisation d'ondes électromagnétiques ou d'un couplage de champ réactif dans la portion de fréquence radio du spectre pour communiquer en direction ou en provenance d'une étiquette à travers différents schémas de modulation et d'encodage, et cela en vue de lire de façon exclusive l'identité d'une étiquette radiofréquence ou d'autres données stockées sur elle ». La Commission a également rappelé son intérêt pour la technologie RFID dans sa Communication au Parlement Européen, au Conseil, au Comité économique et social et au Comité des régions sur « L'identification par radiofréquence (RFID) en Europe : vers un cadre politique, COM (2007) 96 final.

permettant le contrôle à distance des individus grâce à des processus ubiquitaires, opaques et automatiques[20] de croisement de données présumées exactes.

Ce premier volet sécuritaire paraîtrait quelque peu Orwelien s'il n'était accompagné de mesures destinées à garantir les droits fondamentaux des personnes concernées, en particulier leur droit au respect de la vie privée. A ce sujet, l'article 61.1 du Traité de Lisbonne rappelle que *« l'Union constitue un espace de liberté, de sécurité et de justice dans le respect des droits fondamentaux [...] »*. Loin d'être une profession de foi purement formelle, cette exigence semble avoir largement été prise à cœur par les institutions. Outre les nombreuses dispositions relatives à la protection des données à caractère personnel dont regorgent les textes législatifs susmentionnés,[21] la matière fait l'objet d'un maillage législatif fort complexe en droit européen. Les directives 95/46/CE[22] et 2002/58/CE[23] s'appliquent aux domaines relevant du pilier communautaire, une proposition de décision-cadre[24] est en cours de négociation afin de couvrir les matières relevant du 3ème pilier,[25] la convention d'application de l'accord de Schengen[26] contient des dispositions spécifiques sur la protection des données applicables au Système d'information Schengen, la convention Europol[27] contient entre autres les règles relatives à la transmission de données à caractère personnel par Europol à des États et des instances tiers et la décision créant Eurojust[28]

[20] La Commission prévoit de mettre en place un système d'entrée-sortie dans l'UE au moyen de « barrières automatiques ». Les voyageurs de bonne foi et les ressortissants de l'UE qui possèdent un passeport électronique pourraient faire l'objet d'une vérification automatisée à leur arrivée via un dispositif qui effectuerait une comparaison entre les identifiants biométriques du voyageur d'une part, et les données biométriques intégrées dans les documents de voyage ou dans une base de données d'autre part. Voy. la Communication de la Commission, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », op. cit.

[21] Voy. par exemple les articles 6, 7 et 17 de la proposition de Décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité, précitée ; les articles 8 et 9 de la Décision-cadre 2006/960/JAI, précitée ; les articles 24 à 32 de la Décision-cadre 2006/960/JAI, précitée ; l'article 4 du Règlement (CE) nº 1030/2002, précité et l'article 4 du Règlement (CE) nº 2252/2004, précité.

[22] 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 du 23.11.1995, p. 31–50.

[23] Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JO L 201 du 31.7.2002, p. 37–47.

[24] Une proposition de Décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, COM (2005) 475 final, est d'ailleurs actuellement en cours de négociation.

[25] Pour avoir un aperçu des difficultés relatives à la détermination des champs d'application respectifs de la Directive 95/46/CE et la proposition de Décision-cadre, voy. *Dumortier/Poullet* [15].

[26] Convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des Etats 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 C 239 du 22.09.2000, p. 19.

[27] Articles 104 à 118 de la Convention sur la base de l'article K.3 du traité sur l'Union européenne portant création d'un Office européen de Police (Convention Europol), JO C 316 du 27.11.1995, p. 2.

[28] Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, JO L 63 du 06.03.2002, p. 1.

prévoit les dispositions du règlement intérieur d'Eurojust relatives au traitement et à la protection des données à caractère personnel.[29]

Tant le volet sécuritaire que celui relatif à la protection des données font donc l'objet d'une attention toute particulière de la part des institutions chargées de concrétiser l'espace de liberté, de sécurité et de justice. Depuis le traité d'Amsterdam, « droits fondamentaux » et « sécurité » sont ainsi devenus les deux termes principaux de l'équation qu'ont pour mission de solutionner les institutions européennes dans le respect des valeurs démocratiques chères à l'Europe.

Dans cet esprit, un groupe de travail (ci-après « Future Group »[30]) a été mis sur pied par les ministres de l'intérieur et de l'immigration en vue de conseiller les institutions pour préparer le programme de travail post-La Haye. Afin de résoudre l'épineuse question des liens et rapports que doivent entretenir entre eux les concepts de « droits fondamentaux » et de « sécurité », le « Future Group » recourt à la métaphore de la « balance ». Dans son rapport, le groupe propose ainsi de « préserver le modèle européen dans le domaine des affaires intérieures en mettant *en balance* mobilité, sécurité et vie privée ».[31]

Certes, ce groupe n'est pas l'inventeur du concept de la « balance » dans le domaine qui nous intéresse, la notion faisant malheureusement partie du langage politique communautaire depuis quelques années.[32] Nous restons cependant abasourdis de voir figurer, dans un document d'orientation officiel, la référence à la « balance »—un instrument de mesure du poids—comme outil permettant de résoudre la délicate équation impliquant « droits fondamentaux » et « sécurité ».

[29]Nous ne prétendons pas être exhaustif dans l'énonciation des normes appelées à régler d'une manière ou d'une autre l'ensemble des aspects particuliers de la protection des données à caractère personnel dans l'espace de liberté, de sécurité et de justice.

[30]Le « Future Group » est un groupe de travail informel mis en place en 2007, à Dresde, par les ministres de l'intérieur et de l'immigration en vue de préparer l'avenir de l'espace européen de justice, de liberté et de sécurité. La raison d'être du groupe fut de rédiger un rapport politique contenant des recommandations qui serviront de « source d'idées » à la Commission européenne et aux Etats membres dans la conception des politiques dans le domaine des affaires intérieures après 2010.

[31]Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy, précité, p. 17. Selon le groupe,

> one priority for each proposal based on the post-Hague Programme (...) will be the reflection on how to balance mobility, security and privacy in a proportionate way. There is a need to overcome the stereotype of seeing security, mobility and privacy as opposing concepts which exclude each other. Therefore, under the post-Hague Programme, an intensive public debate including a substantial inter-institutional discussion involving the European and national parliaments will have to be launched on how to address the current equilibrium in a way that allows for significantly improved security, at the same time as equally enhanced privacy and mobility.

Son rapport contient d'ailleurs non moins de 16 occurrences de cette notion.

[32]En 2004, M. Frattini, Commissaire en charge de l'espace de JLS déclarait que *« new balances must be found between privacy and security »* (SPEECH/04/549 disponible à l'adresse europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/04/549&format=HTML&aged=1&language=EN&guiLanguage=en). Le 7 septembre 2005, la présidence britannique de l'Union européenne rédigeait déjà un document de travail intitulé *« Liberty and security, striking the right balance »* . Utilisant à nouveau la métaphore de la balance, la Commission européenne lança un programme intitulé *« Security and safeguarding Liberties »* au sein des perspectives financières 2007–2013 (disponible à l'adresse http://ec.europa.eu/justice_home/funding/intro/funding_security_en.htm).

Dans la présente contribution, nous ne referons pas le travail des autorités de contrôle et n'examinerons pas, en tant que telle, la conformité de l'utilisation de RFIDs et de la biométrie dans l'espace JLS avec les normes européennes de protection des données à caractère personnel. Notons toutefois que tant le CEPD[33] que le Groupe de l'article 29[34] ont d'ores et déjà fait connaître leurs positions à propos de l'utilisation de ces technologies par les autorités publiques.[35]

Notre propos consistera plutôt à rappeler, dans un premier temps, que les droits fondamentaux ont été conçus à l'origine comme autant de limites que de finalités de l'exercice du pouvoir par les autorités publiques (2.) et que l'ensemble de ces droits découlent d'une valeur incommensurable reconnue à l'être humain : sa dignité. Nous exposerons ensuite en quoi la généralisation de l'authentification et l'identification biométriques dans le cadre de l'espace JLS peut aller à l'encontre de cette valeur fondamentale (3.). Nous conjuguerons alors le droit à la protection de la vie privée et le droit à la protection des données à caractère personnel à la lumière de cette dignité

[33]Le CEPD (Contrôleur européen de la protection des données) est une autorité de contrôle indépendante dont l'objectif est de protéger les données à caractère personnel et la vie privée et de promouvoir les bonnes pratiques dans les institutions et organes de l'UE.

[34]Le groupe dit « de l'article 29 » est un organe consultatif européen indépendant sur la protection des données et de la vie privée placé auprès de la Commission européenne, composé de représentants de chacune des autorités de protection des données de l'Union européenne. Le groupe a été établi en vertu de l'article 29 de la Directive 95/46/CE. Ses missions sont définies à l'article 30 de la Directive 95/46/CE.

[35]En ce qui concerne le Groupe de l'article 29, voy. notamment l'avis n° 4/2007 sur le concept des données à caractère personnel, l'avis 6/2005 sur les propositions de Règlement du Parlement européen et du Conseil (COM (2005) 236 final) et de Décision du Conseil (COM (2005) 230 final) sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), et sur une proposition de Règlement du Parlement européen et du Conseil sur l'accès des services des États membres chargés de l'immatriculation des véhicules au système d'information Schengen de deuxième génération (SIS II) (COM (2005) 237 final), l'avis 3/2005 sur la mise en oeuvre du Règlement du Conseil (CE) No 2252/2004 du 31 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, l'avis 2/2005 sur la proposition de Règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (COM (2004) 835 final), le document de travail sur les questions de protection des données liées à la technologie RFID (WP 105), l'avis 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système Européen d'information sur les visas (VIS), le Document de travail sur la biométrie (WP 82). En ce qui concerne le CEPD, voy. notamment, l'Opinion du 16 septembre 2008 sur « the proposal for a Council Decision on the establishment fo the European Criminal Record Information System (ECRIS) in application of Article 11 of Framework Decision 2008/XX/JHA », l'Avis du 26 mars 2008 concernant la proposition de Règlement modifiant le Règlement (CE) n° 2252/2004 du Conseil établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres, l'Avis du 20 décembre 2007 sur la Communication de la Commission au Parlement européen, au Conseil, au Comité Economique et Social et au Comité des régions intitulée « L'identification par radiofréquence (RFID) en Europe : vers un cadre politique », l'Avis du 19 décembre 2007 sur l'initiative de la République fédérale d'Allemagne, en vue de l'adoption d'une décision du Conseil concernant la mise en oeuvre de la décision 2007/. . ./JAI relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière, l'Avis du 20 janvier 2006 sur la proposition de Décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des Etats membres compétentes en matière de sécurité intérieure et par Europol aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, l'Avis du 19 octobre 2005 sur trois propositions concernant le système d'information Schengen de deuxième génération (SIS II).

fondatrice avant d'examiner en quoi l'utilisation des RFIDs et de la biométrie à des fins d'identification peuvent porter atteinte à ces droits (4.). Enfin, nous conclurons que le concept de « balance vie privée-sécurité » relève d'un langage inapproprié par rapport à l'esprit des déclarations protectrices des droits de l'Homme. En effet, il ne peut y avoir immixtion des autorités publiques dans l'exercice du droit à la vie privée que pour autant que celle-ci constitue une ingérence digne et proportionnelle dans une société démocratique. Ce postulat mérite certainement d'être rappelé au regard de l'utilisation généralisée de RFIDs et de procédés d'identification et d'authentification biométriques par les pouvoirs publics dans un contexte d'interopérabilité et d'interconnexion croissant des bases de données (5.).

2 Le sens des droits de l'homme : la limite et la finalité de l'exercice du pouvoir

Lorsque l'on écrit sur des problématiques touchant aux droits de l'Homme, il n'est sans doute jamais inutile de rappeler leur sens normatif et le rôle qu'ils sont destinés à jouer dans une société démocratique.

Ecrivant à l'occasion du cinquantième anniversaire de la Déclaration universelle des droits de l'Homme (ci-après DUDH), Michael Ignatieff a pu affirmer que ces derniers apparaissent comme « le principal article de foi d'un monde qui ne croit presque à plus rien ».[36] Suite à la seconde guerre mondiale, la méconnaissance et le mépris des droits de l'Homme qui « ont conduit à des actes de barbarie qui révoltent la conscience de l'humanité »,[37] les 58 Etats Membres qui constituaient alors l'Assemblée générale des Nations Unies adoptent la DUDH, texte fondateur qui inspirera tant la Convention Européenne des droits de l'Homme (ci-après « CEDH ») que la Charte Européenne des Droits Fondamentaux. Dès l'origine, ils apparaissent comme des droits fondamentaux inhérents à l'existence même des êtres humains.[38] De plus,—et c'est là d'une importance cruciale pour notre propos—, même si leur opposabilité peut être étendue à d'autres personnes,[39] les droits de l'Homme sont à

[36] *Ignatieff* [24], p. 6.

[37] Selon le second considérant de la DUDH, « la méconnaissance et le mépris des droits de l'homme ont conduit à des actes de barbarie qui révoltent la conscience de l'humanité et que l'avènement d'un monde où les êtres humains seront libres de parler et de croire, libérés de la terreur et de la misère, a été proclamé comme la plus haute aspiration de l'homme ».

[38] *Gewirth* [20], p. 1 ; *Donnelly* [14], p. 9, qui définit les droits de l'homme comme un ensemble de droits universels appartenant de manière égale à toutes les personnes, exclusivement en raison de leur nature d'êtres humains. Voy. également *Haarscher* [22], p. 168.

[39] Depuis *Young, James and Webster c. Royaume Uni* (du 13 août 1981), la Cour EDH reconnaît l'effet horizontal de la CEDH. (Voir §49 : « Although the proximate cause of the events giving rise to this case was [an agreement between an employer and trade unions], it was the domestic law in force at the relevant time that made lawful the treatment of which the applicants complained. The responsibility of the respondent State for any resultant breach of the Convention is thus engaged on this basis », cité par De Schutter, 2000) Voir aussi, notamment, X et Y c. Netherlands, 8978/80 (1985) Cour EDH (du 26 mars 1985), Series A, vol. 91 : « although the object of Article 8 (art. 8) is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference : in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (see the Airey judgment of 9 October 1979, Series A no. 32,

l'origine des droits dont le respect s'impose essentiellement à l'Etat.[40] A cet égard, les droits de l'Homme ont d'abord été conçus comme un principe de *limitation* du pouvoir étatique. Ces droits ont en effet été interprétés comme autant de garanties de la liberté individuelle par rapport aux ingérences de l'Etat, lequel—on s'en était aperçu—avait tendance à devenir totalitaire lorsqu'il pouvait laisser libre cours à ses immixtions. Par conséquent, ainsi que l'atteste le troisième considérant de la DUDH, la violation des droits de l'Homme par les gouvernants est depuis considérée comme le plus sûr indice *« de tyrannie et d'oppression »*.[41] Enfin, les droits de l'Homme ont également été interprétés comme une *finalité* du pouvoir étatique[42] en ce que les autorités publiques se voient assignées la tâche d'assurer la jouissance effective de ces droits.[43]

C'est dans cette perspective que les droits de l'Homme ont été conçus et doivent encore être interprétés[44] : ils sont la limite, la finalité principale, sinon le fondement même de l'association politique. En ce sens, les droits de l'Homme sont la consécration du principe selon lequel le Pouvoir et les politiques qui en découlent doivent être au service de l'Homme.

Or, ainsi que nous l'avons déjà fait remarquer, le programme de travail de l'espace JLS semble être de plus en plus axé sur la « balance » entre deux « intérêts » considérés comme également importants, à savoir le respect des droits fondamentaux, d'une part, et le désir de sécurité de l'autre. Il convient cependant de rappeler avec force, qu'au contraire du droit au respect de la vie privée,—protégé notamment par l'article 8 CEDH—, un droit fondamental à la sécurité ne fait l'objet d'aucune consécration juridique.

Bien sûr, outre le droit au respect de la vie privée, l'organisation politique a également le devoir d'assurer à chacun le droit *« à la sûreté de sa personne »*.[45] Cependant, il importe de signaler que ce droit à la sûreté signifie toute autre chose qu'un droit à la sécurité. Il implique, entre autres, un devoir pour l'organisation politique

p. 17, para. 32). These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves ».

[40] *Kervegan* [26], p. 644, soulignant que « la thématique des droits de l'individu est le contrecoup de l'affirmation de l'Etat et de son empire sur les individus ».

[41] Selon le 3ème considérant de la DUDH, « il est essentiel que les droits de l'homme soient protégés par un régime de droit pour que l'homme ne soit pas contraint, en suprême recours, à la révolte contre la tyrannie et l'oppression ».

[42] *Gerard* [19], p. 28.

[43] *Tugendhat* [39], p. 362–363 suggérant que les droits de l'homme, en tant que droits moraux au sens fort, impliquent l'exigence de créer un Etat chargé d'assurer leur effectivité. Voy. également dans ce sens, *Wildt* [41], p. 134 et 142. *T. Pogge* soutient pour sa part que les droits de l'homme, en tant que droits moraux, requièrent la création d'un ordre institutionnel assurant leur satisfaction. Voy. *Pogge* [30], p. 51–54.

[44] Rappelons que la Convention Européenne des Droits de l'Homme de 1950 se considère elle-même comme une première mesure propre à assurer la *« la garantie collective de certains des droits énoncés dans la Déclaration universelle »* et que la Charte Européenne des Droits Fondamentaux réaffirme *« les droits qui résultent de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales »* . . . Par conséquent, la Charte des Droits Fondamentaux se situe dans la même perspective que celle de la Déclaration de 1948.

[45] Voy. art. 3 de la DUDH.

d'assurer à chaque être humain de ne pas être arrêté ni détenu arbitrairement. A cet égard, il intéressant de relever que, paradoxalement, l'effectivité de ce dernier droit est rendue moins certaine suite à l'utilisation des technologies biométrique et RFID, particulièrement lors de périodes troubles. Notons, par exemple, que Marc Rotenberg a vivement critiqué la récente initiative militaire des Etats-Unis visant à utiliser des scanners mobiles afin de collecter les empreintes digitales et les iris de centaines de milliers d'iraquiens dans le but de les profiler. Selon ce dernier, *"the new system of biometric identification and secret profiles raises the very real possibility of future reprisals and killings on a far more widespread basis"*.[46] S'il est vrai que la situation politique actuelle en Irak diverge fortement du contexte européen, il n'en a toutefois pas toujours été ainsi. Rappelons, en effet, que sous l'occupation française durant la seconde guerre mondiale, tout comme en Irak actuellement, de nombreuses personnes avaient eu la vie sauve en utilisant de fausses identités. Or, comme nous le verrons plus bas, l'utilisation généralisée d'identifiants biométriques et de technologie RFID dans les documents de voyage couplée à des bases de données interconnectées rend bien plus difficile la dissimulation de l'identité et peut donc faciliter les contrôles discriminatoires ainsi que la détention arbitraire.

Quant à la « sécurité », celle-ci n'a jamais été conçue comme un « droit » ayant un « poids » équivalent à ceux consacrant, par exemple, la dignité et le respect de la vie privée. Deux raisons suffisent à justifier cette conception. Non seulement un « droit à la sécurité » serait susceptible de multiples interprétations contradictoires,[47] mais plus fondamentalement, dans la logique des déclarations fondamentales, c'est *par* le respect de l'ensemble des droits civils, politiques et socio-économiques qu'elles proclament que celles-ci visent à assurer à l'Homme la sécurité civile, politique et socio-économique qui lui revient. La sécurité et la paix *par* la liberté, tel est le credo des droits de l'Homme.[48]

C'est cette logique que renverse Antonio Vitorino, ancien Commissaire européen en charge de la Justice et des Affaires intérieures, lorsqu'il déclare que « la sécurité ne se limite pas à la répression de la criminalité : c'est un moyen pour atteindre la liberté ».[49] Il est d'une importance cruciale pour la démocratie que la métaphore de la « balance » ne conduise pas à confondre la fin et les moyens : c'est par l'assurance étatique de la jouissance effective de ses droits que l'Homme peut espérer vivre en paix et en sécurité, et non le contraire.

En adhérant aux instruments de protection des droits de l'Homme, c'est à cet engagement qu'ont souscrit les institutions européennes. Tant dans la conception que dans la mise en œuvre de leurs politiques, elles ont pour obligation de respecter les droits de l'Homme en tant que limite et fondement du pouvoir afin que la finalité de celui-ci reste au service de l'Homme et de ses droits. C'est pourquoi elles doivent s'atteler à atteindre leur objectif de sécurité *par* le respect effectif des droits à la dignité et au respect de la vie privée, au risque de confirmer la thèse bien connue

[46] Voy EPIC, http://epic.org/privacy/biometrics/epic_iraq_dtbs.pdf.

[47] Parle-t-on de sécurité sociale, politique, économique, culturelle, psychique, juridique ou physique ?

[48] Voy. notamment le préambule de la CEDH selon lequel *« les libertés fondamentales constituent les assises mêmes de la justice et de la paix dans le monde »*.

[49] Voy. http://ec.europa.eu/archives/commission_1999_2004/vitorino/index_en.htm.

d'Agamben et de Carl Schmitt selon laquelle l'« état d'exception » est la véritable source du droit.[50]

3 La dignité humaine : l'Homme en tant que fin en soi

Si les droits de l'Homme sont reconnus en 1948 à tous *« les membres de la famille humaine »*,[51] c'est parce qu'ils sont un ensemble de valeurs et d'intérêts dont le respect est jugé indispensable pour garantir la dignité humaine. L'homme ayant cruellement démontré sa capacité aux pires excès, il était important de rappeler solennellement et avec force le respect que mérite tout être humain du seul fait qu'il est être humain.[52] C'est cet objectif que poursuivent le préambule de la Charte de l'ONU qui réaffirme sa *« foi dans les droits fondamentaux de l'homme, dans la dignité et la valeur de la personne humaine [...] »* et l'article 1er de la DUDH selon lequel *« tous les êtres humains naissent libres et égaux en dignité et en droits »*. C'est également dans cette tradition que s'inscrit la Charte européenne des droits fondamentaux lorsqu'elle proclame en son article 1er que *« la dignité humaine est inviolable. Elle doit être respectée et protégée »*. De manière non équivoque, ces textes considèrent la dignité humaine comme le fondement des autres droits.[53]

Bien que la notion de dignité ne fasse l'objet d'aucune définition légale, elle connaît néanmoins une histoire longue de près de neuf siècles qui permet de la cerner quelque peu. La formulation d'un attribut humain fondamental en termes de *dignitas* trouve en effet sa source dans la pensée de la Renaissance.[54] Elle réapparait au

[50] Voy. *Agamben* [1] et *Schmitt* [38]. Selon *Schmitt*, « Est souverain celui qui décide de la situation exceptionnelle » et « il est impossible d'établir avec une clarté intégrale les moments où l'on se trouve devant un cas de nécessité (Notfall) ni de prédire, dans son contenu, ce à quoi il faut s'attendre dans ce cas ».

[51] Le premier considérant de la DUDH stipule que « la reconnaissance de la dignité inhérente à tous les membres de la famille humaine et de leurs droits égaux et inaliénables constitue le fondement de la liberté, de la justice et de la paix dans le monde ».

[52] En incorporant dans le droit international positif des normes minimales de protection des droits de l'Homme, les rédacteurs de la Charte de l'ONU et de la Déclaration universelle des droits de l'Homme ont voulu éviter que ne se répètent les horreurs de la seconde guerre mondiale, symbole d'une violation massive et d'une ampleur sans précédent de la dignité humaine.

[53] Quant à la CEDH, si elle ne contient pas de références explicites à la « dignité humaine » en tant qu'objectif moteur, il semble néanmoins logique de présumer que sa philosophie est cohérente avec la défense de la « dignité humaine » selon les mêmes principes que les autres instruments internationaux relatifs aux droits de l'Homme. Cette déduction s'appuie sur l'adhésion aux valeurs et objectifs de la Déclaration universelle des droits de l'Homme affirmée dans le préambule de la CEDH et sur les décisions fréquentes de la Cour européenne des droits de l'Homme, dont la portée est générale et qui sont révélatrices des objectifs généraux de la Convention. Ainsi, dans l'affaire *Pretty contre Royaume-Uni*, la Cour a conclu que *« la dignité et la liberté de l'homme sont l'essence même de la Convention »*. De même, dans l'affaire *Gündüz contre Turquie*, la Cour a jugé que *« la tolérance et le respect de l'égale dignité de tous les êtres humains constituent le fondement d'une société démocratique et pluraliste »*.

[54] Le mot « dignité » en français est attesté vers 1155. Voy. *Rey* [34], p. 604. Il dérive du latin *dignitas*, lui-même traduction du grec *axia* que l'on traduit d'habitude par valeur ou *axiôma*, utilisé par Aristote pour « axiome », « principe premier de la raison », « ce qui est approuvé dès qu'énoncé ». De même racine, *axios*, que l'on peut traduire par « digne », signifie plus fondamentalement encore « ce qui a du poids par soi-même », « ce qui entraîne par son propre poids », ou encore « ce qui a de la valeur par soi-même ». Voy. *Fierens* [17], p. 10.

Moyen-Age en 1487 lorsque Jean Pic de la Mirandole écrit son essai *De Hominis Dignitate* qui constitue sans doute la première grande affirmation de la dignité humaine.[55] Au XVIIe siècle, c'est Pascal qui reprend le thème,[56] mais c'est surtout Kant, *« l'homme de droit »*[57] selon Jean Lacroix, qui prépare le mieux la notion juridique de dignité et dont la conception nous intéresse particulièrement pour notre propos, tant ce philosophe fut une source d'inspiration non négligeable pour les auteurs de la DUDH.[58]

Selon Kant,[59]

> dans le règne des fins, tout a un prix ou une dignité. Ce qui a un prix peut être aussi bien remplacé par quelque chose d'autre à titre d'équivalent ; au contraire, ce qui est supérieur à tout prix, ce qui par suite n'admet pas d'équivalent, c'est ce qui a une dignité (...) mais ce qui constitue la condition qui seule peut faire que quelque chose est une fin en soi, cela n'a pas seulement une valeur relative, c'est à dire un prix, mais une valeur intrinsèque, c'est-à-dire une *dignité*.[60]

Dans cette perspective, lorsque la DUDH reconnaît la dignité à l'Homme, elle s'oppose à ce que celui-ci se voit attribuer une valeur relative et par conséquent mesurable. Ainsi, la dignité humaine impose à l'Etat une *limite* fondamentale : celle de toujours considérer l'Homme comme une fin en soi ayant une valeur intrinsèque et absolue. Que penser, dès lors, de l'utilisation par les pouvoirs publics de la biométrie (du grec *bios* signifiant « vie » et *metron*, « mesure ») et de RFIDs à des fins de contrôle des frontières et de surveillance généralisée ?

Rappelons que la biométrie[61] consiste en la *mesure* des éléments physiques, comportementaux et génétiques des êtres humains en vue de les traduire en identifiants uniques, permanents (ils restent pratiquement inchangés au cours de la vie d'une personne) et universels (ils sont valables dans tous les contextes). Au sein de l'espace JLS, l'objet de la biométrie est donc de mesurer l'Homme de manière systématique afin de permettre sa comparaison à un « équivalent » (une empreinte digitale, une

[55] *Pic de la Mirandole* [29]. A cette époque, *Pic de la Mirandole* est aux prises avec les censeurs romains. Le texte représente un élément de sa défense. En résumé, pour Pic, la dignité de l'homme tient à sa liberté. Il n'y a pas d'abord une nature humaine, mais un mouvement, une sorte de pouvoir natal par lequel l'homme décide et réalise son essence. C'est dire que l'homme ne naît pas homme mais le devient, comme s'il était son propre créateur.

[56] Voy. *Fierens* [17], p. 11. « Pascal, en quête de la grandeur de l'Homme à travers sa misère même, affirmera un principe universel en ce sens qu'il vaut pour tous les hommes, et un principe particulier en ce sens qu'il différencie l'homme de toutes les autres créatures : « l'Homme est visiblement fait pour penser, c'est toute sa dignité et tout son mérite ». « Toute la dignité de l'homme est dans la pensée, mais qu'est ce que cette pensée ? Qu'elle est sotte ». « Ce n'est pas de l'espace que je dois chercher ma dignité, mais c'est du règlement de ma pensée ». « Toute notre dignité consiste donc en la pensée ».

[57] *Lacroix* [27], p. 66.

[58] Voy. par exemple l'article 1er de la DUDH qui rappelle que les être humains sont *« doués de raison et de conscience »,* conditions essentielles, selon Kant, pour que l'Homme puisse être responsable de ses actes.

[59] Kant revient au sens le plus originel de la dignité, le sens grec de « valeur en soi », sans équivalent ».

[60] *Kant* [25], p. 160–162. C'est Kant qui souligne.

[61] Biométrie : technologie d'identification ou d'authentification qui consiste à transformer les caractéristique biologiques, morphologiques et comportementales d'une personne comme les empreintes digitales, l'empreinte de la rétine, de l'iris, de la voix, la forme du visage et de la main en une empreinte numérique.

image faciale, un échantillon ADN) dans le but de poursuivre un intérêt sécuritaire par une identification réputée plus « fiable ».

De leur côté, les RFIDs permettent d'assigner diverses informations uniques à des objets—parfois sensibles comme les passeports—et de les lire à distance, de manière ubiquitaire et opaque, transformant petit à petit les voyageurs en des « antennes » émettant automatiquement des informations standardisées sans nécessairement le savoir. En tant que tels, les RFIDs ont ainsi tendance à remplacer l'Homme, à *titre d'équivalent,* comme vecteur principal d'informations.

Dans le cadre de l'espace JLS, la convergence de ces deux technologies peut dès lors avoir pour conséquence le *remplacement* des facultés participatives et narratives de l'Homme par l'interrogation systématique de « capteurs » transmettant automatiquement des informations perçues comme incontestables car liées à l'unicité d'une personne grâce à la *mesure* des parties inchangeables de son corps (bios). Dans cette perspective, l'utilisation combinée de ces technologies à des fins de contrôle aux frontières peut faire courir des risques sérieux à un bon nombre de droits fondamentaux reconnus « à tous les membres de la famille humaine »,[62] citoyens européens ou non, en particulier ceux au respect de la vie privée, « de circuler librement et de choisir sa résidence à l'intérieur d'un Etat »[63] et « de quitter tout pays, y compris le sien, et de revenir dans son pays ».[64]

Certes, la lutte contre la criminalité et l'immigration illégale peuvent être considérés comme étant des objectifs étatiques légitimes, mais l'on peut néanmoins s'interroger sur la dignité du moyen utilisé qui pourrait aboutir au remplacement généralisé des facultés participatives et narratives de l'Homme par des processus d'échanges automatiques d'informations liées à la *mesure* des caractéristiques uniques de ceux-ci. La dignité de l'Homme ne peut être le prix, la *mesure* du désir de sécurité, puisqu'elle en est dépourvue.

La question est d'autant plus concrète étant donnée la *généralisation* de l'utilisation des technologies biométriques et RFID dans les passeports et les bases de données liées à l'immigration. En ce qui concerne ces dernières, rappelons que le système d'information sur les visas (VIS) peut contenir des données relatives à 70 millions de personnes, parmi lesquelles des empreintes digitales. De son côté, le système d'information Schengen (SIS) contenait 22 millions d'entrées au 1er janvier 2008, dont des empreintes digitales. Enfin, dans la seule année 2006, EURODAC a traité 165 958 séries d'empreintes digitales de demandeurs d'asile, 41 312 séries d'empreintes digitales de personnes ayant franchi les frontières irrégulièrement et 63 341 séries d'empreintes digitales de personnes arrêtées alors qu'elles se trouvaient en séjour irrégulier sur le territoire d'un État membre.[65]

Au vu de la généralisation des techniques biométriques et RFID, l'on peut légitimement se demander si ce sont encore les politiques européennes de lutte contre

[62] Voy. le Préambule de la DUDH.

[63] Art. 13.1 de la DUDH.

[64] Art. 13.2 de la DUDH.

[65] Commission européenne, communiqué de presse, « La base européenne de données biométriques continue de garantir une gestion efficace du régime d'asile européen commun », IP/07/1347, 18 septembre 2007.

la criminalité et contre l'immigration illégale qui sont au service de l'Homme ou si, au contraire, ce n'est pas l'Homme qui devient le moyen de réalisation de celles-ci. Si l'on peut admettre que l'identification biométrique d'un être humain n'a pas pour vocation de le ramener à ses identifiants, son objectif premier est toutefois de déterminer ou de vérifier l'identité réelle ou prétendue d'un individu par ses identifiants corporels *afin* de lui appliquer les politiques appropriées et *« de prendre les mesures adéquates »*.[66] L'Homme devient ainsi le moyen de la fin politique sécuritaire lors même que, dans la philosophie des droits de l'Homme, c'est sur lui que cette fin politique devrait être axée.

En effet, selon Kant, si l'humanité est par elle-même une dignité c'est parce que « l'Homme ne peut être traité par l'homme, comme un simple moyen, mais il doit toujours être traité comme étant aussi une fin. C'est précisément en cela que consiste sa dignité (la personnalité) ».[67]

Pour Kant, la dignité de l'Homme en tant que fin en soi implique donc également le respect de sa « personnalité ». Or, dans un contexte d'interconnexion et d'échanges accrus d'informations permettant de confronter les caractéristiques physiques d'un individu à des bases de données de manière instantanée par des procédés informatiques, la biométrie contient en germe le risque d'un glissement de l'identification à la réalisation de *« background checks »* contrôlant les comportements, les conduites et donc la *personnalité* des Hommes par le biais de données corporelles objectivées. Dans ce contexte, l'adjonction de capteurs RFID permettant une lecture ubiquitaire et quasi-automatique—parfois invisible et souvent opaque—d'informations d'identité prétendument infaillibles réduit encore la participation *active* et *narrative* de l'Homme au profit de ce qui est présumé être. Au sens sartrien, l'Homme *est,* il n'*existe* plus. Enfermé dans un canevas de données, l'Homme n'est plus considéré comme une fin en soi ayant *activement* une « personnalité », une *« ipséité »*,[68] c'est-à-dire une « identité » en tant que sujet réfléchi et narrateur participant à la construction de sa biographie. Au contraire, la biométrie peut avoir pour effet d'instrumentaliser le corps en le transformant en un *moyen* objectivable de connaissance de sa personnalité *présumée* dans le but de lui appliquer la politique sécuritaire appropriée. La personnalité *active* et *narrative* de l'Homme court dès lors le risque accru d'être emprisonnée

[66] Communication de la Commission, *« Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne »* , COM (2008) 69 final, *op. cit.*, p. 9.

[67] *Kant* [25].

[68] La distinction entre *« mêmeté »* et *« ipséité »* provient de *P. Ricoeur*. Selon ce dernier, le terme « identité » appliqué à un être humain peut désigner en français deux réalités différentes. La première concerne son corps dans son objectivité : à travers l'espace et le temps, à travers les lieux et les âges de sa vie, ce corps reste le même : c'est ce que l'auteur appelle la *« mêmeté »*. C'est cet aspect que la biométrie permet de cerner : depuis la conception grâce à l'analyse génétique, jusqu'à la mort grâce aux données corporelles identifiantes obtenues de diverses manières—notamment grâce à des particularités morphologiques et à la photographie du visage. L'autre réalité concerne le vécu d'existence, par un sujet humain conscient et réfléchi. C'est le « soi-même », en anglais le *« self »*. On peut la désigner, pour la distinguer de la précédente, par le terme *« ipséité »*, tiré du latin « ipse ». De ce point de vue, c'est le corps-sujet et non seulement le corps-objet qui est en cause, le corps tel qu'il se vit de l'intérieur et non pas tel qu'il se voit de l'extérieur. Cette réalité est certes subjective, mais c'est elle qui importe d'un point de vue éthique, car c'est elle qui rend possible l'exercice de la liberté. Voy. Comité Consultatif National (français) d'Ethique pour les Sciences de la Vie et de la Santé, Avis n° 98, *« Biométrie, données identifiantes et droits de l'homme »,* du 26 avril 2007, p. 7.

dans un réseau de données identifiant sa *« mêmeté »* dont il ne pourra s'échapper par narration, lors même que la dignité fondatrice de sa liberté réside dans son *« ipséité »*.

Les récentes propositions de la Commission pour une *« stratégie de gestion intégrée des frontières »*[69] illustrent parfaitement les risques de dérives liés à la confiance aveugle en l'identification biométrique et dans les bases de données. Concrètement, la Commission prévoit l'instauration d'un *« système d'enregistrement des entrées et sorties »*[70] des voyageurs et considère l'installation de barrières automatiques à la frontière qui rendrait possible une vérification automatisée de l'identité des voyageurs, sans intervention des gardes-frontières. Un appareil lirait les données biométriques figurant dans les documents de voyage ou stockées dans un système ou une base de données, et les comparerait aux identifiants biométriques du voyageur. Ce nouveau système « pourrait fonctionner sur la même plateforme technique que le SIS II et le VIS, en exploitant les synergies avec le système de correspondance biométrique (BMS), en cours de développement, qui pourrait constituer la base commune pour le système d'entrée/sortie, le VIS et le SIS II ».[71] De cette manière, ces barrières automatiques pourraient opérer automatiquement des contrôles[72] *« dans le SIS et les bases de données nationales »*[73] afin de vérifier que les voyageurs ne sont pas de nature à compromettre l'ordre public, la sécurité intérieure, la santé publique ou les relations internationales de l'un des États membres.

Outre l'authentification des voyageurs en tant que telle, l'utilisation de la biométrie permettrait donc l'automatisation—au dépend des facultés narratives des êtres humains concernés—des procédures de consultation du SIS et de *« bases de données nationales »* dont on ignore la nature précise dans le contexte d'interopérabilité ambiant. Or, lorsque l'on sait que Mr. et Mme. Moon[74] ont du engager des procédures judiciaires durant 12 ans pour obtenir l'effacement des enregistrements illégitimes de leurs signalements du SIS, on comprend aisément en quoi l'aptitude narrative des êtres humains s'oppose à l'automatisation de la gestion des frontières quand des dé-

[69] Voy. Communication de la Commission au Conseil et au Parlement européen—*« Vers une gestion intégrée des frontières extérieures des états membres de l'Union européenne »*, COM (2002) 233 final, 7 juin 2002, la Communication de la Commission du 13 février 2008 au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée « Examen de la création d'un système européen de surveillance des frontières (EUROSUR) » COM (2008) 68 final—non publié au Journal officiel. Voy. également la Communication de la Commission, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », COM (2008) 69 final, *op. cit.* Pour un commentaire de ces communications, Voy. *Guild/Carrera/Geyer* [21], disponible à l'adresse http://shop.ceps.eu/BookDetail.php?item_id=1622.

[70] Communication de la Commission, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », COM (2008) 69 final, *op. cit.*, p. 8.

[71] *Ibidem*, p. 9.

[72] En vertu du code frontières Schengen, la consultation du SIS est systématique pour les ressortissants de pays tiers mais ne peut être qu'aléatoire dans le cas des jouissant du droit communautaire à la libre circulation.

[73] Communication de la Commission, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », COM (2008) 69 final, *op. cit*, p. 4.

[74] Sur cette affaire, voy. *Brouwer* [9], disponible à l'adresse http://www.libertysecurity.org/IMG/pdf_The_Other_Side_of_Moon.pdf.

cisions aussi importantes qu'une interdiction de territoire, un renvoi ou une expulsion sont en jeu.[75]

Bien sûr, il est généralement admis que pour pouvoir assurer ses missions d'intérêt général, l'Etat puisse reconnaître ses propres membres grâce à des données identifiantes extérieures, qui sont des données corporelles en quelque sorte rendues publiques, celles que nous appelons « état civil ». Elles permettent d'identifier dans l'espace public chaque citoyen par sa *« mêmeté »* et de le désigner : « c'est bien lui ».[76] Mais au vu de la multiplication et de la diversification des données d'identification biométriques, des techniques de collecte et de traitement de celles-ci, du paradigme sécuritaire de l'espace JLS basé sur une interopérabilité, une interconnexion—voire une centralisation—des bases de données et sur un échange accru d'informations grâce au principe de disponibilité, on peut s'interroger légitimement sur l'espace de liberté laissé à la personne, dans son *« ipséité »*. Là est la question éthique centrale dont nous examinons les implications juridiques dans les sections suivantes.

Ayant à présent rappelé que les droits de l'Homme constituent la *limite* et le *fondement* de l'action étatique et que cette limite et ce fondement imposent aux autorités de toujours respecter la dignité de l'Homme en tant que fin en soi, nous examinons dans la section suivante les conséquences qu'entraîne le respect de cette dignité fondatrice au niveau du droit à la protection de la vie privée et du droit à la protection des données à caractère personnel.

4 Le respect de la vie privée au regard de la dignité humaine : un engagement en faveur de l'autonomie par le biais de l'intégrité informationnelle

4.1 Le droit au développement social et relationnel de la personnalité

Si la dignité humaine a acquis une importance considérable au sein du cadre conceptuel qui régit les droits de l'Homme c'est parce que ceux-ci ont été conçus, dès l'origine, comme un bouclier de droits visant à empêcher toute entrave à la dignité humaine. Par conséquent, un droit de l'Homme particulier tel que celui qui protège le respect de la vie privée peut être qualifié de *« droit au respect de la dignité »*[77] dans la mesure où son objet est la défense indirecte de la dignité inhérente à l'Homme.

Un tel engagement en faveur de la dignité est intrinsèquement bidimensionnel,

[75] A cet égard, les récentes propositions de la Commission poussent d'autant plus à la prudence lorsqu'elles prévoient que le système d'entrée/sortie vérifierait également le respect des délais de séjour des ressortissants de pays tiers et enregistrerait un signalement *« accessible aux autorités nationales lorsque la durée de séjour autorisée dans l'UE est écoulée »*. Un tel enregistrement automatisé de signalements peut, en effet, comporter un risque d'atteinte à la libre circulation de certaines catégories de personnes telles que les ressortissants de pays tiers introduisant par la suite une demande de regroupement familial, les ressortissants de pays tiers entrés sur base d'un visa touristique mais ayant obtenu par la suite le statut de résident de longue durée ou encore les demandeurs d'asile se trouvant légitimement sur le territoire de l'UE durant l'examen de leur demande d'asile. Pour toutes ces catégories de personnes, il est fort à parier que la lutte entre narration et traitement automatisé de signalements sur base de données biométriques ne sera pas gagnée d'avance.

[76] Comité Consultatif National (français) d'Ethique pour les Sciences de la Vie et de la Santé, *op. cit.*

[77] *Feldman* [16], notamment p. 689.

> il y a d'une part son aspect absolu (le caractère moralement mauvais de la cruauté et de l'humiliation) et de l'autre un engagement en faveur de l'épanouissement humain (peut-être moins évident, mais tout aussi essentiel). Ces deux aspects sont liés, dans la mesure où chacun d'entre eux découle d'un engagement en faveur de la dignité humaine, qui se manifeste quant à lui dans des actes de compassion envers autrui. Sous sa forme prohibitive, le concept nous interdit la dépersonnalisation de nos semblables par des actes dégradants. Le côté positif qui met l'accent sur le développement et la réussite personnels, considère les droits de l'Homme comme étant radicalement pluralistes, dans le cadre de l'hospitalité envers les autres (et non la simple tolérance) qu'exige l'éthique qui le sous-tend. Considérés comme un tout, les droits de l'Homme sont par conséquent une idée qui, dans le même temps, nous protège en tant que personnes et nous permet de nous épanouir.[78]

En tant qu'engagement envers l'Homme comme fin en soi, la dignité humaine comporte donc un aspect négatif, à savoir l'interdiction de la dépersonnalisation de l'Homme—la condamnation de la réduction de l'Homme à sa *« mêmeté »*—etun aspect positif consistant en un devoir de promotion de l'épanouissement et de l'émancipation de l'Homme dans sa liberté, son *« ipséité »*.

Conçu comme un *« droit au respect de la dignité »*, le droit à la vie privée est également lui-même tout naturellement bidimensionnel en soi. Ainsi, Agre a pu définir le droit au respect de la vie privée comme « la possibilité pour l'individu de construire sa propre personnalité à l'abri de contraintes excessives ».[79]

Tant l'aspect négatif du droit à la protection de la vie privée,—l'absence de contraintes déraisonnables imposées par l'Etat ou des tiers—, que son aspect positif,—la possibilité de construire sa personnalité—, découlent de l'engagement fondamental en faveur de la dignité humaine. Loin d'être deux aspects poursuivant des objectifs normatifs distincts, ces deux versants soutiennent la même valeur finale, à savoir l'autonomie de l'Homme conçue comme « la capacité de l'Homme à maintenir et à développer sa personnalité d'une manière qui lui permette de participer pleinement à la société sans être poussé à conformer ses pensées, ses croyances, ses comportements et ses références aux pensées, croyances, comportements et préférences de la majorité ».[80] Cette valeur d'autonomie personnelle a été reconnue explicitement par la Cour EDH comme étant le principe interprétatif de l'article 8. Dans l'arrêt Pretty, la Cour considère ainsi que « bien qu'il n'ait été établi dans aucune affaire antérieure que l'article 8 de la Convention comporte un droit à l'autodétermination en tant que tel, [. . .] la notion d'autonomie reflète un principe important qui sous-tend l'interprétation des garanties de l'article 8 ».[81]

Cette autonomie personnelle ne doit cependant pas être perçue comme encourageant une « retraite et une indépendance radicales de la personne vis-à-vis de son

[78] *Gearthy* [18], p. 140–141.

[79] *Agre/Rottenberg* [2], p. 3.

[80] *Rouvroy/Poullet* [35], p. 15.

[81] Cour EDH, *Pretty c. Royaume-Uni* du 29 avril 2002, §61.

environnement social mais bien plutôt comme l'autonomie d'une personne radicalement intégrée dans la société, vivant et communiquant avec d'autres personnes ».[82] Ce droit à une vie privée relationnelle et sociale a été confirmée par la Cour EDH dans l'arrêt Niemietz, lorsqu'elle estime qu'il serait trop restrictif de limiter le droit au respect de la vie privée « à un « cercle intime » où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables ».[83]

Dans le même sens, la Cour EDH a jugé dans l'affaire Pretty que le droit au respect de la vie privée inclut « le droit au développement personnel et le droit d'entretenir des rapports avec d'autres êtres humains et le monde extérieur ».[84] Loin de constituer deux droits distincts, le droit au développement personnel et le droit d'entretenir des relations avec les autres sont intimement liés ainsi que le rappelle la Cour qui évoque le droit « d'assurer le développement de la personnalité de chaque individu *dans* ses relations avec ses semblables ».[85]

Ce droit à l'épanouissement dans les relations sociales est également applicable aux ressortissants de pays tiers.[86] En effet, en se prononçant dans une affaire d'éloignement d'étrangers, le juridiction strasbourgeoise a considéré qu'en ayant « été éloignées du pays où elles avaient, sans interruption depuis la naissance, noué des relations personnelles, sociales et économiques qui sont constitutives de la vie privée de tout être humain »,[87] les requérantes avaient subi une ingérence dans leur « vie privée » au sens de l'article 8.

Dans la même perspective, dans l'arrêt Boultif, la Cour a estimé que « le refus de renouveler son autorisation de séjour en Suisse constitue une ingérence dans l'exercice par l'intéressé de son droit au respect de sa vie familiale, au sens de l'article 8 §1 de la Convention »[88] au motif qu'exclure une personne d'un pays où vivent ses parents proches peut constituer une ingérence dans le droit au respect de la vie familiale.

Ainsi, le respect effectif du droit à la vie privée exige de la part des autorités publiques non seulement le devoir de s'abstenir de restreindre la liberté considérée, mais également de prendre certaines mesures—telles que l'octroi d'un visa ou le renouvellement d'un permis de séjour. L'immigrant entré clandestinement sur le territoire d'un pays d'Europe comme le candidat réfugié débouté peuvent ainsi alléguer qu'un ordre d'expulsion—voire le refus de régulariser leur situation—constitue une ingérence dans leur vie privée

Enfin, la Cour a estimé qu'autonomie personnelle et développement personnel sont liés à l'identité, entendue comme le médium par excellence par lequel l'Homme

[82] *Ibidem*, p. 15.

[83] Cour EDH, *Niemietz c. Allemagne* du 16 décembre 1992, §29.

[84] Cour EDH, *Pretty c. Royaume-Uni* du 29 avril 2002, §61.

[85] Cour EDH, *Botta c. Italie* du 24 février 1998, §32.

[86] Pour une étude plus générale de la jurisprudence de la Cour EDH relative à l'application de l'article 8 à des ressortissants de pays tiers, voy. *Docquir* [13], p. 921.

[87] Cour EDH, *Slivenko c. Lettonie* du 9 octobre 2003, §93.

[88] Cour EDH, *Boultif c. Suisse* du 2 août 2002, §40.

noue des relations avec les autres. Comme telle, l'identité est ainsi protégée sur le terrain de l'article 8, la Cour déclarant que « le respect de la vie privée exige que chacun puisse établir les détails de son identité d'être humain et que le droit d'un individu à de telles informations est essentiel du fait de leurs incidences sur la formation de la personnalité ».[89]

C'est pourquoi, dans l'arrêt Smirnova,[90] alors que la Cour devait se prononcer sur l'incidence de la privation de passeport sur le respect du droit à la vie privée, elle estima

> que les citoyens russes doivent, dans leur vie quotidienne, faire état de leur identité particulièrement souvent, même pour accomplir des tâches aussi courantes que celles d'échanger de la monnaie ou d'acheter des billets de train. Le passeport interne est également nécessaire pour des besoins plus cruciaux, comme trouver un emploi ou recevoir des soins médicaux. Aussi la privation de son passeport a-t-elle représenté, pour Y.S., une ingérence continue dans sa vie privée.[91]

L'octroi conditionnel ou la privation d'un titre de séjour tout comme l'intégration de données relatives aux droits de séjour ou à l'identité d'un individu dans des bases de données publiques[92] (EURODAC, VIS, etc.) constituent donc, en eux mêmes, des ingérences dans la vie privée des personnes concernées, qui, pour être justifiables aux yeux de la Convention, doivent être conformes au triple critère de l'article 8, §2.

Dans le contexte de l'utilisation de technologies biométriques et RFIDs dans l'espace JLS à des fins d'identification et de régulation de flux migratoires, cette réalité juridique mérite certainement d'être rappelée. Ainsi pour être conformes aux exigences de la CEDH, la généralisation d'identifiants biométriques dans l'ensemble des bases de données liées à l'immigration et dans les titres de séjour ainsi que l'utilisation de RFIDs dans ces documents se doit de ne pas exacerber de manière disproportionnée l'ingérence que constituent, déjà en eux-mêmes, les documents et bases de données liées à l'identité et à l'immigration.

Or, ainsi que le rappelle le CEPD, les données biométriques sont particulières du fait de certaines de leurs caractéristiques vantées, à savoir « la possibilité d'une identification quasi-certaine (elles sont uniques pour chaque individu), leur permanence (elles restent pratiquement inchangées au cours de la vie d'une personne) et leur universalité (les mêmes « éléments » physiologiques se retrouvent chez tous les individus) ».[93] Ces prétentions d'universalité, de pertinence et de permanence sont

[89] Cour EDH, *Mikulić c. Croatie* du 7 février 2002, §54 ; voy. également *Gaskin c. Royaume-Uni*, arrêt du 7 juillet 1989, série A n° 160, p. 16, §39.

[90] Cour EDH, *Smirnova c. Russie* du 24 juillet 2004.

[91] *Ibidem*, §97.

[92] Dans l'arrêt Rotaru, la Cour rappelle que « tant la mémorisation par une autorité publique de données relatives à la vie privée d'un individu que leur utilisation et le refus d'accorder la faculté de les réfuter constituent une ingérence dans le droit au respect de sa vie privée garanti par l'article 8 §1 de la Convention ». Cour EDH, *Rotaru c. Roumanie*, 4 mai 2000, §46.

[93] CEPD, Avis du 23 mars 2005 sur la proposition de Règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (COM (2004) 835 final, p. 7).

cependant largement surfaites et loin d'être absolues, rendant, par conséquent, les traitement basés sur des « preuves » biométriques hautement sensibles du fait de la confiance excessive qui peut leur être conférée.

D'une part, le caractère d'universalité des données biométriques doit être nuancé étant donné que la proportion de personnes dont les empreintes digitales ne sont pas exploitables pourrait s'élever jusqu'à 5% (en raison d'empreintes digitales illisibles ou faisant entièrement défaut).[94] Par conséquent, si l'on peut estimer à quelque 20 millions le nombre de demandeurs de visas en 2007, « près d'un million de personnes ne seront pas en mesure de suivre la procédure d'enregistrement « normale », ce qui aura des conséquences évidentes au niveau des demandes de visas et au niveau des contrôles aux frontières ».[95]

Enfin, l'identification biométrique étant, par définition, un processus statistique, il serait exagéré de considérer qu'elle assure une « identification exacte » des personnes. L'authentification de personnes, par empreinte digitale, est ainsi affectée d'un taux d'erreur normal de 0,5 à 1% ;

> par conséquent, le pourcentage des rejets injustifiés (False Rejection Rate) du système de contrôle aux frontières extérieures oscillera entre 0,5 et 1%. Ce pourcentage varie en fonction d'un seuil déterminé par la politique des autorités compétentes en matière de gestion des risques (qui correspond à l'établissement d'un équilibre entre le nombre de personnes rejetées par erreur et acceptées par erreur).[96]

Loin d'être purement formelles, les craintes liées une importance accrue ou exagérée accordée aux preuves biométriques ont d'ores et déjà été vérifiées dans certaines affaires, un avocat de Portland, par exemple, ayant été emprisonné en 2004 pendant deux semaines parce que le FBI avait établi que ses empreintes digitales correspondaient à des empreintes trouvées dans le cadre des attentats de Madrid sur un sac plastique ayant contenu le détonateur.

Pour ces raisons, le Groupe de l'article 29 a déjà exprimé des réserves

> concernant la constitution d'une base de données centrale dans laquelle seraient enregistrées les données biométriques de tout étranger demandeur d'un visa ou d'un titre de séjour à des fins de contrôles ultérieurs des immigrants illégaux, quand ces données seraient de telle nature qu'elles porteraient sur des éléments dont toute personne laisse des traces dans la vie quotidienne.[97]

Cette prise de position du Groupe ne semble cependant pas avoir troublé la Commission outre mesure dans sa proposition, déjà évoquée, de mettre en place un système d'entrée/sortie aux frontières extérieures. Non seulement des « barrières automatiques » authentifieraient l'identité des individus par l'examen de leur document

[94] *Sasse* [37], p. 7, et United States General Accounting Office, Technology Assessment, « Using Biometrics for Border Security », GAO-03-174, novembre 2002.

[95] CEPD, Avis du 23 mars 2005, *op. cit.*, p. 7.

[96] *Ibidem*, p. 8.

[97] Groupe de l'article 29, Avis n° 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information Visas (VIS), p. 8.

de voyage biométrique et effectueraient des contrôles dans des bases de données européennes et nationales, mais le système vérifierait également le respect des délais de séjour des ressortissants de pays tiers et enregistrerait un signalement « accessible aux autorités nationales lorsque la durée de séjour autorisée dans l'UE est écoulée ».[98] Un tel traitement automatisé comporterait, selon nous, un risque sérieux d'atteinte au droit à la vie privée de l'ensemble des ressortissants de pays tiers qui pourraient se voir interdire l'accès à un territoire, et par voie de conséquence à un réseau de relations sociales, sur base d'informations erronées. De plus, le système pourrait avoir pour conséquence d'enregistrer illégitimement des signalements pour dépassement de délai de séjour chez certaines catégories de personnes, pourtant en situation régulière, telles que les ressortissants de pays tiers introduisant par la suite une demande de regroupement familial, les ressortissants de pays tiers entrés sur base d'un visa touristique mais ayant obtenu par la suite le statut de résident de longue durée ou encore les demandeurs d'asile se trouvant légitimement sur le territoire de l'UE durant l'examen de leur demande d'asile. Serait ainsi menacé le principe consacré au considérant 2 de la Directive 95/46, selon lequel

> les systèmes de traitement de données sont au service de l'homme ; (...) ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus.

Non seulement le droit à la protection de la vie privée, lu à la lumière des principes de dignité et d'autonomie, implique-t-il le respect de l'épanouissement de chacun dans ses relations avec ses semblables et subséquemment une protection contre les ingérences disproportionnées des autorités dans la liberté d'aller et de venir des individus, mais il impose également, selon certains, un droit de pouvoir se comporter avec les autres de manière contextualisée.[99] Nous arguons, dans les sections suivantes, que c'est à l'égard de cette dimension contextuelle du droit à la protection de la vie privée que les RFID et la biométrie suscitent les plus importantes interrogations.

4.2 Le droit à intégrité contextuelle

Selon un arrêt précurseur de la Cour constitutionnelle allemande,[100] l'autodétermination de l'Homme présuppose que celui-ci

> continue à disposer de sa liberté de décider d'agir ou de s'abstenir, et de la possibilité de suivre cette décision en pratique. Si l'individu ne sait pas prévoir avec suffisamment de certitude quelles informations le concernant sont connues du milieu social et à qui celles-ci pourraient être communiquées, sa liberté de faire des projets ou de décider sans être soumis à aucune pression est fortement limitée.

[98] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, *« Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne »* , op. cit., p. 9.

[99] *Nissenbaum* [28].

[100] Cour constitutionnelle, 15 décembre 1983, *EuGRZ*, 1983, p. 171.

Cette nécessité d'autodétermination contextualisée permettant aux Hommes de décider de manière autonome et informée a également été mise en lumière par la Cour EDH, notamment dans l'arrêt Guerra,[101] considérant que les familles concernées auraient du avoir accès à une information pertinente relative aux inconvénients en termes de pollution environnementale pour exercer librement leur droit à la vie privée dans leur choix d'élire domicile près d'un complexe industriel.

Dans l'esprit de la Cour, l'autodétermination de l'Homme suppose donc une liberté de poser des choix *en contexte* avec un minimum d'ingérence afin de s'épanouir dans ses relations avec les autres. Il en résulte que la manière dont l'Homme exerce sa liberté décisionnelle d'agir ou de s'abstenir ainsi que sa liberté d'épanouissement et de développement personnel dépendent du contexte géographique, temporel, social, culturel et intersubjectif dans lequel il évolue. Il y a près de quarante ans, Barker proposait déjà son concept de « behavior setting »[102] pour désigner des modèles de conduite déterminés par une structure composée d'éléments physiques et sociaux qui interfèrent avec des données culturelles propres au contexte. La relation entre espace et comportement, à laquelle on préfère souvent le terme d'« action », est envisagée aujourd'hui comme une conduite adaptative qui se traduit par le choix d'une option s'inscrivant dans un système de contraintes et d'opportunités. Ainsi les « lieux » sont vus, non seulement comme des localisations dans l'espace mais aussi comme des catégorisations de l'expérience qui permettent à l'individu de se représenter les actions qu'il est susceptible de mener dans cet espace et les moyens qu'il a d'y parvenir d'après la manière dont sont connues et appréhendées les opportunités et les contraintes contextuelles.[103]

Dans cette perspective, le droit à la protection de la vie privée implique le droit pour l'*« être multiple »* de pouvoir faire évoluer son « soi » (et sa liberté décisionnelle d'agir et de s'abstenir) d'après des normes relationnelles plus ou moins formelles selon la situation contextuelle envisagée. Une telle protection de la contextualisation des comportements participerait, selon nous, à l'effectivité du « droit à pouvoir mener sa vie comme on l'entend avec un minimum d'ingérence »[104] tel qu'il a été consacré par le Conseil de l'Europe. En tant qu'instrument au service de l'autonomie, le droit au respect de la vie privée doit donc aussi être compris comme un « droit à l'intégrité contextuelle »[105] comprenant, le cas échéant, un droit à l'*imprévisibilité* inter-contextuelle.[106]

[101] Cour EDH, *Guerra c. Italie*, 19 février 1998.

[102] *Barker* [7].

[103] Voy. notamment *Canter* [10] ; *Prohansky/Fabian/Kaminoff* [32] ; *Altman/Low* [3].

[104] Résolution 428 du Conseil de l'Europe « portant déclaration sur les moyens de communication de masse et les droits de l'homme » du 23 janvier 1970.

[105] *Nissenbaum* [28].

[106] Cette garantie d'intégrité contextuelle ne doit cependant pas être comprise dans une perspective individualiste mais comme un outil garantissant le fonctionnement démocratique et vivace de la société. En effet, la protection de l'imprévisibilité inter-contextuelle a pour but de sauvegarder toute une série de comportements, postures, attitudes, expressions et modes de vie qui, sans être illégaux ni dommageables à autrui, sont simplement inhabituels, originaux, bizarres, saugrenus ou tout bonnement « différents », et qui à l'aune d'une mondialisation accélérée se doivent d'être protégés au titre du pluralisme nécessaire à l'effectivité de la démocratie. En 1920, Zamiatine avait déjà perçu toute la richesse et la vivacité de ce

A cet égard, l'utilisation de RFIDs par les pouvoirs publics pose un certain nombre de questions. Les principales inquiétudes quant au respect de l'« intégrité contextuelle » découlent de la nature même de la technologie RFID qui *parle pour nous* et qui consiste, en tant que telle, en une « technologie infrastructurelle » composée d'un certain nombre d'éléments reliées en *réseau,* à savoir l'étiquette, le lecteur, la base de données de référence et la base de données dans laquelle les données produites par l'association étiquette-lecteur sont conservées. Ainsi que le relève la Commission,

> les RFID ne sont pas de simples étiquettes ou codes-barres électroniques. Lorsque les dispositifs sont reliés à des bases de données ou des réseaux de communication, comme l'Internet, cette technologie offre un moyen très puissant de fournir de nouveaux services et applications *dans pratiquement n'importe quel environnement*.[107]

Pour cette raison, les RFID sont considérés par l'Union internationale des télécommunications (UIT) comme la passerelle vers une nouvelle phase de développement de la société de l'information, souvent appelée « Internet des objets », dans laquelle l'Internet ne met plus seulement en relation ordinateurs et terminaux de communication, mais quasiment tous les objets de notre environnement quotidien, qu'il s'agisse de vêtements, de biens de consommation, de cartes de transports ou même d'objets plus sensibles tels que les documents de voyage.

On parle d'ailleurs, notamment au sujet des RFIDs, d'*« ubiquitous computing »* ayant plusieurs caractéristiques. Il s'agirait tout d'abord d'

> une technologie de l'ubiquité dans la mesure où les terminaux peuvent être placés partout et dès lors enregistrer les faits les plus anodins de notre vie quotidienne, nos déplacements, nos hésitations, notre consommation domestique. Cette technologie est ensuite une technologie largement invisible (« calm technology ») dans un double sens : elle fonctionne de manière opaque, invisible (nous ne connaissons pas le circuit d'information sous-tendant le fonctionnement de la puce : qui la lit ? Quand ? Quelles informations ? Pour qui ?), mais également elle apparaît comme le prolongement naturel même de notre action (la porte s'ouvre et l'ordinateur s'allume) mettant les choses à notre service. Enfin, cette technologie est dite « apprenante » (« learning technology »). Ses applications ont souvent en effet pour caractéristique d'adapter leur fonctionnement aux données obtenues de par leur utilisation.[108]

Les caractéristiques d'opacité et d'ubiquité de la technologie RFID, liées à des risques évidents en matière de sécurité, font craindre, tout d'abord, un manque de

qu'il appelle les « hérésies », selon celui-ci « le monde se développe uniquement en fonction des hérésies, en fonction de ceux qui rejettent le présent, apparemment inébranlable et infaillible. Seuls les hérétiques découvrent des horizons nouveaux dans la science, dans l'art, dans la vie sociale ; seuls les hérétiques, rejetant le présent au nom de l'avenir, sont l'éternel ferment de la vie et assurent l'infini mouvement en avant de la vie ». Zamiatine [42], p. 11.

[107] Communication de la Commission au Parlement Européen, au Conseil, au Comité économique et social et au Comité des régions sur « L'identification par radiofréquence (RFID) en Europe : vers un cadre politique, COM (2007) 96 final, p. 1.

[108] *Poullet/Rouvroy* [31], p. 5.

transparence pouvant donner lieu à une collecte et à un traitement d'informations à l'insu des personnes concernées, mais aussi, plus fondamentalement, une atteinte à l'intégrité contextuelle de ces informations. En effet, l'aspect « communication sans fil » de l'étiquette, ainsi que la capacité de lecture hors de portée visuelle qui la caractérise, rendent floues les limites traditionnelles de *« l'espace personnel »,* se traduisant généralement selon Hall[109] par la distance physique qui s'établit entre des personnes.

Un tel danger de dé-contextualisation des informations a été mis en lumière par des chercheurs du Réseau d'Excellence FIDIS[110] dans leur déclaration de Budapest[111] présentant les résultats de leur étude sur les Documents de Voyage à Lecture Automatique (MRTD—Machine Readable Travel Documents). Selon ceux-ci,

> à la différence des documents d'identité habituels, les DVLA européens peuvent être lus et interceptés jusqu'à une distance de 10 mètres du porteur, de façon transparente et sans contrôle interactif ; cette faiblesse est encore aggravée par un contrôle d'accès susceptible d'être contourné ou attaqué, de sorte qu'un tiers, autorisé ou non, peut y avoir accès pour identifier le porteur et le ficher afin de, par exemple, suivre à la trace les touristes dans un pays étranger.[112]

Après avoir mis en exergue les multiples voies de piratage (man in the middle, vol de clef, système basique de contrôle d'accès vulnérable à une attaque en force brute, clonage aisé des RFID contenus dans les documents de voyage, etc.), l'analyse des chercheurs de FIDIS conclut que « la combinaison de ces menaces et de ces faiblesses met sérieusement en cause la sécurité et la sphère privée des citoyens européens ; ceci est tout particulièrement vrai si l'on considère le déploiement à grande échelle des DVLA actuels et leur longue durée de validité (jusqu'à 10 ans) ».[113] Ces mises en garde en matière de sécurité ont depuis lors été actualisées par plusieurs chercheurs[114] démontrant, par exemple, que les passeports belges de première génération—c'est à dire ceux émis jusqu'en juillet 2006—ne sont munis d'aucun mécanisme de sécurité et ont pu être lus à distance en quelques secondes à l'insu de leur porteur. Quant aux passeports seconde génération, émis depuis juillet 2006 et équipés de mesures de sécurité—le Basic Access Control (BAC)—, les chercheurs ont également démontré qu'ils ont pu accéder au contenu de ceux-ci après seulement une heure.[115] Pour continuer dans la même veine, Jeroen van Beek, chercheur en sécurité à l'Université d'Amsterdam, a également pu lire et cloner les puces RFID de deux passeports biométriques britanniques avant d'y remplacer les photos par celles d'Osama Ben Laden

[109] *Hall* [23].

[110] FIDIS (*Future of Identity in the Information Society* ou Futur de l'Identité dans la Société de l'Information) est un réseau d'excellence créé dans le cadre du sixième programme cadre de l'Union Européenne.

[111] La déclaration de Budapest de septembre 2006 est disponible à l'adresse http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_on_MRTD.fr.pdf.

[112] *Ibidem*, p. 2.

[113] *Ibidem*, p. 3.

[114] Voy. notamment *Avoine/Kalach/Quisquater* [4].

[115] *Avoine/Kalach/Quisquater* [5].

et de Hiba Darghmeh, morte en 2003 dans un attentat.[116] Enfin, le Groupe de l'article 29 a lui-aussi identifié le risque de dé-contextualisation des informations liées à l'identité estimant que des

> préoccupations s'appliquent lorsque des terroristes seraient en mesure de détecter des nationalités spécifiques dans des foules. L'intrusion dans la vie privée serait encore plus grave quand le dispositif lui-même contient des informations personnelles importantes comme par exemple des renseignements relatifs au passeport ou des informations hautement sensibles.[117]

Insérée dans des documents de voyage, la technologie RFID fait donc courir un risque sévère d'atteinte à l'intégrité contextuelle des informations d'identité des individus en ce qu'elle met ceux-ci dans l'incapacité de dire leur identité, de la circonstancier et de la contextualiser. En ce sens, elle est problématique : les individus ne savent plus ce qu'ils disent, à qui ils le disent, quand ils le disent et où ils le disent.

La dimension contextuelle du droit à la vie privée est non seulement mise en danger par l'utilisation de technologie RFID dans les documents de voyage mais également par la généralisation des éléments biométriques dans ces documents et dans des bases de données telles que le SISII, le VIS et EURODAC. En effet, étant donné que l'Homme fait évoluer son « soi » de manière circonstanciée selon la relation intersubjective envisagée mise en contexte, le reflet de la personnalité de l'Homme (les informations qu'il transmet et celles qui sont stockées et échangées à son propos) est également variable et multiple. L'Homme doit donc avoir la possibilité d'exercer son droit à l'auto-détermination pour décider quelles informations adéquates, pertinentes et non-excessives il divulgue eu égard à ses objectifs et à sa prévision de ce qui est légitimement su de lui dans ce contexte. A cet égard, l'utilisation de la biométrie dans le cadre de l'espace JLS pose un certain nombre de questions que nous analysons dans la section suivante.

4.3 Le droit à l'intégrité informationnelle dividuelle

Alors que le droit à la protection de la vie privée est un droit reconnu à l'Homme, le droit à la protection des données à caractère personnel est conféré à une catégorie de destinataires sensiblement différente, à savoir les « personnes concernées ».[118] Le terme anglais de *« data subjects »* est éclairant à ce propos, tant il tend à mettre en exergue le fait que ce sont les sujets de données—les *sujets* de représentations—qui sont protégés par le droit à la protection des données à caractère personnel. Là où

[116] Voy. Timesonline, 6 août 2008, disponible à l'adresse http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece.

[117] Groupe de l'article 29, Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification), 19 janvier 2005, WP 105, p. 8.

[118] Bien sûr, le droit à la protection des données à caractère personnel poursuit un objectif analogue au droit au respect de la vie privée, la Directive 95/46/CE stipulant expressément que celle-ci a pour objectif *« la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel »*. Le droit à la protection des données à caractère personnel participe ainsi, entre autres, à la garantie de la survivance d'une certaine autonomie nécessaire dans une société démocratique.

le droit à la protection de la vie privée participe à l'émancipation du « soi » humain multiple et potentiellement imprévisible, nous arguons que la protection des données à caractère personnel tend à prémunir les *« personnes virtuelles »*[119]—ou plutôt les *« dividus »*[120] contextuels—de la dé-contextualisation de leurs représentations informationnelles.

Selon Danièle Bouvier, la personne virtuelle peut être vue, d'abord, comme une personne numérique.

> Il s'agit d'un « groupe d'informations nominatives qui circulent dans un réseau, rendant ainsi l'individu concerné présent sous forme incorporelle ». La transformation de la personne physique en nombre, en numéro, c'est-à-dire sa « numérisation », crée une nouvelle logique d'identification qui se caractérise par une domiciliation abstraite où s'exprime une télépersonnalité.[121]

Reprenant la notion de personne virtuelle, les chercheurs du projet FIDIS ont pointé la multiplicité de celle-ci en estimant que *« nowadays, we all have several (partial) identities in our daily life. These identities are based on roles, actions, activities and may vary also depending on the context. New technologies have a direct impact on the very concept of identity »*.[122]

Constatant cet éclatement de la personnalité physique en de multiples personnalités virtuelles, certains auteurs ont dès lors prophétisé la mort de l'individu. Afin d'exprimer ce passage de l'individu à celle du *« dividu »* en contexte informationnel, Deleuze écrit qu'*« on ne se trouve plus devant le couple masse-individu. Les individus sont devenus des « dividuels », et les masses, des échantillons, des données, des marchés ou des « banques »*.[123] Depuis lors, dans leur best-seller mondial « Les Netocrates »,[124] Alexander Bard et Ian Soderqvist ont réutilisé le terme de « dividu ». Selon ceux-ci,

> un individu est un objet indivisible, tandis qu'un « dividu » peut être séparé en différents éléments, puis réassemblé pour former de nouvelles structures. Nous ne sommes plus des êtres « individuels », mais des dividus existant dans des contextes sociaux différents. Et, plus important, nous avons arrêté d'essayer d'être constamment « toujours le même », fidèle à notre « véritable moi ». Au contraire, nous nous délectons à apparaître différents selon les contextes. Nous avons abandonné l'idéal de la personnalité « monopsychique » pour lui préférer celui de la personnalité « schizoïde ». Nous chercherons désormais des consultations en schizanalyse plutôt qu'en psychanalyse. C'est la mort sociologique du sujet cartésien ».[125]

[119] *Bourcier* [8].

[120] *Deleuze* [12].

[121] *Bourcier* [8], p. 865.

[122] FIDIS, deliverable "D 2.13 Virtual Persons and Identities", p. 24.disponible à l'adresse http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.13_Virtual_Persons_v1.0.pdf.

[123] *Deleuze* [12].

[124] *Bard/Soderqvist* [6].

[125] Voy. l'entretien d'Alexander Bard dont les sont recueillis par Rémi Sussan, disponible sur le site www.laspirale.org.

Dans le cadre d'une société de l'information comme la nôtre où l'accès à des lieux, à des services, à des droits sont basés sur des traitements de données contenues dans des banques de données contextuelles, l'« individualité » kantienne—au sens de pôle de subjectivité unique et cohérent—a donc tendance à faire place à des *« dividualités »* multiples—sans pour autant être toujours étanches entre elles—qui résultent des informations traitées *dans* un certain contexte social, relationnel et intersubjectif *pour* un certain objectif contextuel. Dans chaque contexte, chaque dividualité se voit attribuer un identifiant différent (tel numéro de client au supermarché, tel numéro de téléphone professionnel, tel numéro de téléphone privé, tel pseudonyme sur un site de rencontres, tel numéro de dossier de demande d'asile, tel numéro de vignette visa, tel numéro de compte en banque, etc.), lui permettant de construire sa représentation contextuelle dans un mouvement réciproque avec les intervenants du contexte dans lequel elle s'inscrit pour obtenir l'accès à tel lieu, tel service ou tel droit. C'est dans ce passage de l'individualité à la dividualité que nous situons la nécessité d'un droit à la protection des données à caractère personnel assurant un rempart contre la dé-contextualisation informationnelle de représentations dividuelles construites en contexte. En tant que garantie de l'« auto-détermination informationnelle »,[126] la protection des données à caractère personnel participe à la liberté autonomique de l'Homme « de faire des projets ou de décider »[127] sans être soumis à aucune pression exagérée (ce qu'assure le droit à la protection de la vie privée) *par* la garantie qu'elle offre aux « dividus contextuels » (les « data subjects ») de pouvoir « prévoir avec suffisamment de certitude quelles informations le concernant sont connues du milieu social et à qui celles-ci pourraient être communiquées ».[128]

A la lumière de ce principe d'« intégrité informationnelle » peuvent être lues nombre de dispositions des instruments européens de protection des données. Il en va ainsi notamment de l'article 6 b) de la Directive 95/46 selon lequel les données doivent être *« collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités »* exprimant l'idée que les représentations dividuelles ne peuvent être utilisées que dans le cadre d'un contexte déterminé, explicite et proportionné, et que celles-ci ne peuvent être réutilisées dans un contexte incompatible. Il en va de même pour l'article 5 c) d'après lequel les données traitées doivent être *« adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement »* rappelant que les représentations dividuelles ne peuvent être basées que sur des informations strictement nécessaires aux objectifs contextuels. C'est encore le cas pour l'article 5 e) qui stipule que les données ne peuvent être *« conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement »,* lequel article peut être interprété comme procurant aux représentations dividuelles une garantie d'intégrité informationnelle temporelle.

[126] Sur cette notion, voy. *Rouvroy/Poullet* [36].

[127] Cour constitutionnelle, 15 décembre 1983, *EuGRZ*, 1983, p. 171.

[128] *Ibidem*.

En somme, nous voyons le droit à la protection des données comme la garantie d'une certaine « intégrité informationnelle dividuelle » au service du droit au respect à la vie privée, conçu lui-même en tant qu'outil assurant l'« intégrité contextuelle » des Hommes en vue de favoriser les capacités d'autonomie de ceux-ci au nom de leur radicale dignité. C'est précisément cette dimension dividuelle du droit à la protection des données à caractère personnel que l'utilisation d'éléments biométriques dans les documents de voyages et les bases de données liées au contrôle des frontières extérieures remet en question. Nous distinguons deux principaux risques de dé-contextualisation : le premier découle des caractéristiques intrinsèques de l'indentification et de l'authentification biométriques ; le second dérive du cadre institutionnel dans lequel cette technologie est utilisée.

En ce qui concerne le premier risque, il est évident qu'en utilisant les empreintes des parties inchangeables du corps réduites à des codes numériques uniques pour chaque « individu », permanents—car évoluant peu dans le temps—et universels car valables dans l'ensemble des contextes dans lesquels celui-ci évolue, la biométrie *individualise* l'ensemble des dividualités contextuelles et temporelles de l'Homme et risque potentiellement de dé-contextualiser celles-ci. En utilisant des « caractéristiques physiques uniques et particulières d'une personne pouvant—du moins théoriquement—lui être attribuées en tout lieu et en tout temps avec une certitude quasi absolue »,[129] la biométrie contient en germe un risque de « function creep » susceptible de pervertir une méthode d'identification en un système de surveillance dématérialisé portant sur tous les aspects du monde vécu.

Avec la biométrie, on entre dans l'ère de l'interopérabilité maximale et les frontières inter-contextuelles perdent de leur substance. Ce constat est d'autant plus frappant dans le cadre de l'utilisation de la biométrie pour le contrôle des frontières extérieures de l'espace JLS. Alors que traditionnellement, les activités de contrôle se déroulaient dans un espace physique bien délimité et facilement localisable comme la frontière ou la place publique, la biométrisation des contrôles virtualise ces lieux fixes. Or, il convient de remarquer

> que contrairement au monde virtuel qui englobe totalement l'individu, le monde physique ne s'impose pas entièrement à lui. Caractérisé par une structure aléatoire et contingente, il le laisse libre d'entrer ou de ne pas entrer dans son territoire, à l'exemple de l'individu qui décide de ne pas voyager donc de ne pas traverser les frontières, lieux fixes de l'identification et de contrôle. Toutefois, avec la biométrisation des contrôles, une fois entré dans le monde virtuel de l'identification et de surveillance, l'individu n'aura plus la latitude de le quitter. Par l'inscription de ses empreintes biométriques dans les bases de données nationales et transnationales, il entrera dans un monde virtuel de contrôles dont par ailleurs il ne connaît pas vraiment l'existence.[130]

Un second risque de dé-contextualisation découle, non pas de l'utilisation en tant que telle des technologies RFID et biométriques, mais plutôt de la structure institutionnelle au sein de laquelle cette utilisation s'inscrit. Il va de soi que la technologie

[129] Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données élaboré par PRIVATIM, les commissaires suisses à la protection des données, octobre 2006, n° 3.1.2.

[130] *Ceyhan* [11].

ne se réduit pas seulement à un dispositif technique, scientifique et symbolique, mais qu'elle est également conditionnée par le contexte dont elle est le produit. Or, le nouvel espace JLS est structuré autour d'un titre unique servant de base institutionnelle à deux contextes de déploiement de politiques sensiblement différents à savoir d'une part la gestion des flux migratoires et, d'autre part, la lutte contre la criminalité et la coopération judiciaire.[131]

Un sérieux danger de dé-contextualisation des informations traitées au sein de l'espace peut dès lors découler de ce titre institutionnel unique qui peut avoir comme effet, si on n'y prend garde, d'assimiler le demandeur d'asile, le demandeur de visa ou encore l'immigrant illégal à un criminel ayant commis un délit suffisamment grave pour justifier une collaboration transfrontière entre autorités policières nationales. Or, rappelons que dans nombre d'Etats Membres, le séjour en situation irrégulière n'est constitutif d'aucun délit. Tout récemment, le Commissaire aux droits de l'Homme[132] constatait d'ailleurs

> avec une inquiétude grandissante une tendance à soumettre au droit pénal, dans le cadre d'une politique de gestion des migrations, l'entrée et la présence clandestines de migrants. Une telle méthode de maîtrise des déplacements internationaux porte atteinte aux principes établis du droit international. Elle est aussi à l'origine de nombreuses tragédies humaines sans pour autant atteindre sa finalité qui est de maîtriser réellement l'immigration. [...] Cette idée est peut-être populaire chez les xénophobes, mais elle constituerait une mesure rétrograde.[133]

L'assimilation des politiques migratoires et de lutte contre la criminalité ne s'arrête pas à leur institutionnalisation dans un titre unique. En effet, dès le programme de la Haye, le Conseil est d'avis que « si l'on veut assurer une protection optimale de l'espace de liberté, de sécurité et de justice, l'action—au niveau de l'UE comme au niveau national—*doit être multidisciplinaire* et concertée entre les autorités répressives compétentes, en particulier la police, les douanes et la police des frontières ».[134] C'est dans ce contexte que le Conseil européen et le Conseil de l'Union européenne ont tous deux invité à plusieurs reprises la Commission à présenter des propositions visant à accroître l'efficacité et l'interopérabilité des bases de données européennes et à créer entre elles des synergies.

[131] Comme en témoigne la structure du titre V du Traité sur le fonctionnement de l'UE, l'espace de sécurité, de liberté et de justice est structuré autour de trois grands pôles d'action. Un premier chapitre est consacré aux « politiques relatives aux contrôles aux frontières, à l'asile et à l'immigration », un second à la « coopération judiciaire en matière civile » et un dernier à la « coopération policière et judiciaire en matière pénale ». Le nouveau Traité de Lisbonne réunit ainsi, sous un même titre, l'ancien titre IV (visas, asile, immigration et autres politiques liées à la libre circulation des personnes) du Traité CE et l'ancien titre VI (dispositions relatives à la coopération policière et judiciaire en matière pénale) du Traité UE.

[132] Le Commissaire aux droits de l'Homme est une institution indépendante au sein du Conseil de l'Europe ; sa mission est de promouvoir la prise de conscience et le respect des droits de l'homme dans les 47 Etats membres du Conseil de l'Europe.

[133] Commissaire aux droits de l'Homme, Point de vue : « Il est injuste de sanctionner pénalement les migrations », 29 septembre 2008, disponible à l'adresse http://www.coe.int/t/commissioner/Viewpoints/080929_fr.asp.

[134] Programme de La Haye, p. 4.

Poussant à l'extrême la confusion entre les domaines de la gestion de l'immigration et de la lutte contre la criminalité, la Commission a soumis, en 2006, une proposition pour permettre aux autorités des États membres compétentes en matière de sécurité intérieure et à l'Office européen de police (Europol) d'accéder au système d'information sur les visas (VIS) afin de leur permettre de mieux prévenir et détecter des infractions pénales, notamment celles liées au terrorisme.[135]

Exerçant sa compétence d'avis, le CEPD n'a pas manqué de relever le phénomène de dé-contextualisation qu'implique l'accès des services répressifs au VIS en estimant que

> l'octroi aux services répressifs de l'accès à des bases de données relevant du premier pilier, même s'il peut être justifié par la lutte contre le terrorisme, est loin d'être anodin. Il convient de ne pas perdre de vue que le VIS est un système d'information mis au point aux fins de l'application de la politique européenne en matière de visas et non comme instrument de répression. Un accès systématique constituerait en effet une grave violation du principe de limitation de la finalité. Il entraînerait une ingérence disproportionnée dans la vie privée des voyageurs qui ont accepté que leurs données fassent l'objet d'un traitement en vue d'obtenir un visa, et s'attendent à ce que ces données soient collectées, consultées et communiquées uniquement à cette fin.[136]

La tendance n'est pourtant pas prête d'être inversée puisque le Conseil « Justice et affaires intérieures » qui s'est réuni à Luxembourg les 12 et 13 juin 2007 a invité la Commission à présenter dans les plus brefs délais une modification du règlement EURODAC afin de permettre aux services de police et aux services répressifs des États membres ainsi qu'à Europol d'avoir accès, dans certaines conditions, à EURODAC, base de données conçue initialement comme instrument pour l'application du Règlement de Dublin.

5 Conclusion : "*in dubio, pro libertate*"

Tout au long des sections précédentes, nous avons essayé de décrire les diverses dimensions du droit à la vie privée et du droit à la protection des données à caractère personnel auxquelles l'utilisation de la biométrie et des RFIDs dans le cadre de l'espace JLS portent incontestablement atteinte. Nous avons tout d'abord rappelé que le droit au respect de la vie privée comporte le droit de pouvoir développer sa personnalité dans ses relations avec ses semblables et que, par conséquent, l'« identité »

[135] Proposition de Décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, COM (2005) 600 final, Non publié au Journal officiel.

[136] CEPD, Avis du 20 janvier 2006 sur la proposition de Décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des Etats membres compétentes en matière de sécurité intérieure et par Europol aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière (COM (2005) 600 final), p. 2.

et les documents y afférant sont protégés sur le terrain de l'article 8. Ainsi, l'octroi conditionnel ou la privation d'un titre de séjour tout comme l'intégration de données relatives aux droits de séjour ou à l'identité d'une personne dans des bases de données publiques constituent en eux-mêmes des ingérences au droit au respect de la vie privée. Nous avons alors exposé en quoi les technologies biométrique et RFID exacerbaient ces ingérences par les effets de dé-contextualisation informationnelle que celles-ci impliquent. D'une part, l'inclusion de RFIDs dans les documents de voyage peut avoir pour effet de mettre les Hommes dans l'incapacité de dire leur identité, de la circonstancier et de la contextualiser, et ce au mépris de leurs facultés narratives et participatives. Ensuite, l'inclusion d'éléments biométriques dans ces mêmes documents et dans les bases de données relatives aux contrôles aux frontières peut entraîner, on l'a rappelé, une confiance exagérée dans les preuves biométriques pouvant potentiellement entraîner des décisions aussi graves qu'une arrestation ou un renvoi sur base d'informations erronées. Enfin, l'interopérabilité maximale rendue possible grâce à la biométrie attise encore le phénomène de dé-contextualisation informationnelle dans un contexte institutionnel où « criminalité » et « immigration » sont diluées dans un concept unique de « sécurité », attribuant systématiquement des représentations informationnelles stigmatisantes aux ressortissants de pays tiers.

L'ingérence accrue dans le droit à la protection de la vie privée ainsi provoquée par l'utilisation des RFIDs et de la biométrie dans le cadre de l'espace JLS ne fait donc pas de doute. Cependant, faut-il le rappeler, le droit à la protection de la vie privée n'est pas un droit absolu. Dès notre introduction, nous évoquions d'ailleurs la propagation, au sein du monde politique européen, du concept de la « balance » comme outil permettant de résoudre l'équation entre les intérêts de « vie privée » et de « sécurité ». Nous avons toutefois rappelé que cette métaphore keynésienne était contraire à l'esprit des déclarations fondamentales qui fonde l'ensemble des droits de l'Homme sur l'incommensurable dignité de celui-ci. Il ne peut donc être question de « balance » entre un intérêt—aussi légitime soit-il—et un droit fondamental faute de « prix » pouvant lui être associé.

La métaphore de la « balance » peut, en outre, affecter de manière significative l'état de droit basé, nous l'avons rappelé, sur le respect des droits de l'Homme comme *limite* et *fondement* du Pouvoir. Ainsi que le constate Peter Hustinx,[137]

> a message such as : "No right to privacy until life and security are guaranteed" is developing into a mantra suggesting that fundamental rights and freedoms are a luxury that security cannot afford. [...] the Home Secretary of the United Kingdom, Dr John Reid, called for human rights law to be rewritten, stating that "The right to security, to the protection of life and liberty, is and should be the basic right on which all others are based". [...] This position could be potentially dangerous and may produce more problems than it seeks to solve. Not only does it reveal a lack of understanding of the current framework of human rights in general, and data protection legislation in particular, which both enable proportionate measures that are necessary for public security or defence, it also ignores the lessons learned about the abuse of fundamental rights from

[137] Peter Hustinx est le contrôleur européen à la protection des données.

> dealing with terrorism within Europe's borders over the last 50 years. There should be no doubt that effective anti-terror measures can be framed within the boundaries of fundamental rights. It is these rights that need to be protected under all circumstances in a democratic society. In the past examples can be found in different parts of Europe where the failure to protect fundamental rights has served as source of continued unrest rather than ensure safety and stability.[138]

Nous nous rallions à l'analyse du CEPD et souhaitons mettre en exergue que le « principe de précaution » apparu récemment au niveau européen en matière d'environnement ne peut en aucun cas légitimer l'introduction de technologies sécuritaires intrusives et le recours exponentiel aux bases de données, devenues le moyen d'anticipation des comportements « à risque ». Cet univers de « précaution » omniprésente est en effet incompatible avec l'esprit des déclarations fondamentales selon lequel, rappelons-le, les immixtions dans le droit au respect de la vie privée ne sont justifiées, au regard de l'article 8 CEDH, que lorsque celles-ci (A.) poursuivent l'un des buts légitimes visés à l'article 8, §2 et constituent (B.) des ingérences (C.) « nécessaires dans une société démocratique » pour la réalisation de la finalité légitime poursuivie.

A. Tout d'abord, l'article 8, §2 de la CEDH ne permet d'« ingérence » dans le droit fondamental au respect de la vie privée que lorsque celles-ci poursuivent l'une des finalités légitimes énoncées en son sein. Dans le cadre de l'espace JLS, l'utilisation de des technologies RFID et biométrique semble poursuivre deux grandes catégories de finalités différentes à savoir, d'une part, un but de coopération policière et judiciaire, et, d'autre part, une finalité de régulation des flux migratoires. En ce qui concerne la première catégorie, il ne fait pas de doute que la coopération en matière répressive et judiciaire puisse être rangée sous les vocables de *« défense de l'ordre et prévention des infractions pénales »,* de *« sûreté publique »,* voire de *« sécurité nationale »*. Quant à la finalité de régulation des flux migratoires, l'exercice de qualification est plus délicat. Si la protection du *« bien-être économique du pays »*[139] a parfois été invoquée comme but légitime justifiant la régulation des flux migratoires, des recherches sociologiques récentes indiquent toutefois que la main d'œuvre clandestine joue un rôle non négligeable dans le fonctionnement des économies européennes (secteurs de la construction, de la restauration, de l'agriculture).[140] Un débat sur cette question devant la Cour EDH serait le bienvenu.
B. Ensuite, lorsque des intérêts tels que la *« sûreté publique »*, la *« sécurité nationale »,* la *« défense de l'ordre et la prévention des infractions pénales »* ou la protection du *« bien-être économique du pays »* entrent en concours avec le droit au respect de la vie privée, la poursuite de ceux-ci n'est autorisée, *sous conditions*, par la CEDH, qu'au titre d'une « ingérence ». Or, le terme « ingérence » provient à l'origine d'*« ingerere »* qui dès 1362 signifie en langue française *« s'introduire*

[138] CEPD, "Letters to the incoming presidency : fundamental rights are not captives of security", 11 juin 2007, disponible à l'adresse http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2007/07-06-11_Letters_portuguese_presidency_EN.pdf.

[139] Cour EDH, arrêt *Berrehab c. Pays-Bas*, 21 juin 1988.

[140] Voy. *Rea* [33], p. 831, et références citées.

indûment, sans en être requis ou en avoir le droit ».[141] Ce côté très restrictif de la notion d'ingérence est d'autant mieux mis en valeur par sa traduction anglaise *« interference »* du latin « *enterferer* » (*enter*, entre et *ferir*, frapper, dérivé de *forare* : forer, percer) qui signifie aussi bien *« entrechoquer »* que *« percer un trou dans »*. Dans cette perspective, une « ingérence » réalisée au nom d'un des buts légitimes susmentionnés qui *« s'entrechoque »* avec le respect des droits de l'Homme, peut tout au plus avoir comme effet d'y *« percer un trou »*. Au vu de la généralisation de l'identification précise par biométrie et RFID, —dont nous avons démontré les risques—, de la propagation des bases de données contenant des éléments biométriques et de leur interconnexion, on peut dès lors se poser la question de savoir si la condition d'« ingérence » est encore respectée par les autorités européennes. L'ensemble du « maillage » sécuritaire mis en place dans le cadre de l'espace JLS n'a t'il réellement pour effet que de *« percer un trou »* dans les droits à la dignité et au respect de la vie privée des personnes concernées ? La dilatation croissante du « trou » dans le droit à la protection de la vie privée des Hommes, citoyens européens ou non, n'est-il pas un premier symptôme du passage, que nous évoquions plus haut, de la conception d'une « société en paix *par* le respect des libertés » à une « société libre *par* la sécurité » ?

C. Outre cette considération d'ordre étymologique, le principe de proportionnalité exige encore que l'« ingérence » des pouvoirs publics soit « nécessaire » dans une société démocratique. Par cette exigence, la CEDH impose aux autorités l'examen du caractère « nécessaire » de la mesure qu'elles prévoient de mettre en œuvre en vue de parvenir à l'un des buts légitimes énumérés à l'article 8, §2. Dans sa jurisprudence, la Cour Européenne des Droits de l'Homme a estimé que le sens de l'adjectif « nécessaire » était intermédiaire entre, d'une part, « indispensable » et, d'autre part, « admissible », « normal », « utile », « raisonnable » ou « opportun »,[142] étant entendu que le simple opportunisme n'est pas un motif suffisant. Pour être nécessaire, l'ingérence doit encore être justifiée par un « besoin social impérieux »[143] se rapportant à un ou plusieurs buts légitimes. L'action de l'Etat doit en outre se fonder sur « une appréciation acceptable des faits pertinents ».[144] L'examen du caractère « proportionné » de l'« ingérence » commande donc l'analyse d'une triple exigence de « nécessité », de « besoin social impérieux » et de « motifs pertinents et suffisants ».[145] En matière de surveillance, la Cour a ainsi déjà estimé que « le pouvoir de surveiller en secret les citoyens n'est tolérable [...] que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques ».[146] Il s'agit là du « degré minimal de protection voulu par la prééminence du droit dans une société démocratique ».[147] Dans la même perspective, certains auteurs considèrent que « la règle de la proportionnalité postule

[141] Trésor de la Langue Française Informatisé (TLFI), disponible à l'adresse http://atilf.atilf.fr/tlf.htm.

[142] Cour EDH, arrêt *Sunday Times* du 26 avril 1979, série A no 3, §59.

[143] *Ibidem.*

[144] Cour EDH, arrêt *Oberschlick* du 23 juin 1991, série A no 204, §60.

[145] Cour EDH, arrêt *Dudgeon c. Royaume-Uni* du 22 octobre 1981, série A, n°45, §50 à 53.

[146] Cour EDH, arrêt *Rotaru c. Roumanie*, 4 mai 2000, §47.

[147] Cour EDH, arrêt *Kopp c. Suisse* du 25 mars 1998, §75.

> l'exclusivité du moyen : non seulement la limitation de la liberté doit apparaître comme le seul moyen apte à atteindre le but autorisé, mais encore, parmi plusieurs mesures qui peuvent s'offrir à elle, l'autorité doit opter pour la mesure la moins restrictive ».[148]

Au vu de l'inflation législative, déjà mentionnée, dans les domaines qui nous intéressent et du nombre de propositions prescrivant l'utilisation d'éléments biométriques ainsi que l'introduction de la technologie RFID dans les documents de voyages—dont l'importance des risques combinés a été démontrée—, l'on peut légitimement se demander si le principe de proportionnalité—en tant qu'il impose la minimisation des données ainsi que la modération dans le choix de la technologie—a été respecté par les autorités responsables de l'espace JLS.

La complexité et le nombre d'initiatives dans les matières évoquées posent également certains soucis au CEPD qui avoue ne plus toujours être en mesure d'évaluer correctement la proportionnalité des propositions qui lui sont soumises, pour avis, par les autorités. Selon celui-ci,

> regardless of the inherent merits of each proposal, the EDPS is concerned that far reaching proposals implying surveillance of the movements of individuals follow each other at an amazing pace. Many proposals have been or are about to be tabled in this area (SIS II, VIS, review of Eurodac Regulation, access of law enforcement agencies to these systems, PNR, etc.). All these proposed measures are intended to contribute to the monitoring of travellers before and upon entry to the EU (or Schengen) territory. *The sheer number of these proposals and the seemingly piecemeal way in which they are put forward make it extremely difficult for the stakeholders (European and national Parliaments, data protection authorities including EDPS, civil society) to have a full overview*. This limits the possibility to contribute meaningfully. *There is for instance a risk that Data Protection Authorities might find a proposal acceptable only to discover later that it would actually be unacceptable when considered in synergy with the other, more recent proposals*. The EDPS would like to see evidence that there is a master plan for all these initiatives, giving a clear sense of direction. Such a general plan would greatly help to analyse the impact of the totality of these measures on the travellers (in third countries, at entry or within the EU territory) and to design appropriate safeguards.[149]

Face à la complexité de l'analyse de proportionnalité résultant des synergies—parfois voulues, parfois non—entre, d'une part, les différentes propositions législatives, et, d'autre part, les différentes technologies utilisées, il n'y a, selon nous, qu'une réponse démocratiquement acceptable : *« in dubio, pro libertate »*. Les droits et libertés doivent faire l'objet d'une définition extensive, lors que les limitations susceptibles de leur être apportées doivent être interprétés restrictivement afin que la

[148] *Velu/Ergec* [40], p. 120.

[149] CEPD, "Preliminary comments on three Communications from the Commission on border management (COM (2008) 69, COM (2008) 68 and COM (2008) 67)", 3 Mars 2008, p. 3, disponible à l'adresse http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf.

CEDH puisse continuer *« de protéger des droits non pas théoriques ou illusoires, mais concrets et effectifs »*.[150]

Bibliographie

1. Agamben, G.: État d'exception. Homo sacer, Seuil (2003)
2. Agre, P.E., Rottenberg, M. (eds.): Technology and Privacy. The New Landscape. MIT Press, Cambridge (1998)
3. Altman, I., Low, S.M. (eds.): Place Attachment. Plenum, New York (1992)
4. Avoine, G., Kalach, K., Quisquater, J.: Visite guidée du passeport biométrique. In: Dossier RFID, sécurité et vie privée, revue MISC, novembre 2007
5. Avoine, G., Kalach, K., Quisquater, J.: Le passeport biométrique belge recalé au BAC. . .Vos informations personnelles sont en danger!. Disponible à l'adresse http://www.dice.ucl.ac.be/crypto/passport/index_fr.html
6. Bard, A., Soderqvist, I.: Netocracy: The New Power Elite and Life After Capitalism. FT Press, London (2002)
7. Barker, R.: Ecological Psychology. Stanford University Press, Stanford (1968)
8. Bourcier, D.: De l'intelligence artificielle à la personne virtuelle: émergence d'une entité juridique?. Droit Soc. **49**, 847–871 (2001)
9. Brouwer, E.: The other side of Moon—the Schengen information system and human rights: a task for national courts. CEPS Policy Brief No. 288, CEPS, avril 2008
10. Canter, D.: The Psychology of Place. Architectural Press, London (1977)
11. Ceyhan, A.: Enjeux d'identification et de surveillance à l'heure de la biométrie, Cultures & Conflits, 64, hiver 2006. Disponible à l'adresse http://www.conflits.org/index2176.html
12. Deleuze, G.: Post-scriptum sur les sociétés de contrôle. L'autre J. 1 (1990)
13. Docquir, P.-F.: Droit à la vie privée et familiale des ressortissants étrangers : vers la mise au point d'une protection floue du droit de séjour ?. Revue Trimestrielle des Droits de l'Homme 6/2004
14. Donnelly, J.: The Concept of Human Rights. Londres (1985)
15. Dumortier, F., Poullet, Y.: La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union européenne. In: Revue Lamy Droit de l'Immatériel, issue 29, pp. 76–86
16. Feldman, D.: Human dignity as a legal value—Part I (La dignité humaine en tant que valeur juridique, 1ère partie). Public Law (hiver), 682–702 (1999)
17. Fierens, J.: Encombrante dignité humaine. In: Cahiers de la Faculté de droit de Namur; 30 (2002)
18. Gearthy, C.: Can Human Rights Survive? The Hamlyn Lectures 2005 (Les droits de l'homme peuvent-ils survivre ? Les conférences de Hamlyn 2005). Cambridge University Press, Cambridge (2006)
19. Gerard, Ph.: L'esprit des droits—philosophie des droits de l'homme. Publications des Facultés universitaires de Saint-Louis, Bruxelles (2007)
20. Gewirth, A.: The epistemology of human rights. In: Paul, E.F., Paul, J., Miller, F.D. Jr. (eds.) Human Rights. Oxford (1986)
21. Guild, E., Carrera, S., Geyer, F.: The Commission's New Border Package: Does it take us one step closer to a 'cyber-fortress Europe'?. CEPS Policy Brief No. 154, CEPS, Mars 2008
22. Haarscher, G.: Droits de l'homme. In: Raynaud, Ph., Rials, S. (dir.) Dictionnaire de philosophie politique. Paris (1998)
23. Hall, E.T.: La dimension cachée, 1ère éd. Doubleday, Garden City (1966)
24. Ignatieff, M.: Droits de l'homme : la crise de la cinquantaine. Esprit **255–256**, 6–23 (1999)
25. Kant, I.: Fondement de la métaphysique des mœurs (1785)
26. Kervegan, J.-Fr.: Les droits de l'homme. In: Kambouchner, D. Notions de philosophie II. Paris (1995)
27. Lacroix, J.: Kant et le Kantisme. Coll. Que sais-je?, n° 123. Presses universitaires de France, Paris (1969)
28. Nissenbaum, H.: Privacy as contextual integrity. Washington Law Rev. **79**(1), 119–158 (2004)
29. Pic de la Mirandole, J.: Œuvres philosophiques, texte latin, traduction et note par Olivier Boulnois et Giuseppe Tognon. Coll. Epiméthée. Presses universitaires de France, Paris (1993)

[150]Cour EDH, arrêt *Airey v. Ireland* du 9 octobre 1979, §22. Voy. également Cour EDH, arêt *Loizidou v. Turkey* du 23 March 1995.

30. Pogge, T.: The international significance of human rights. J. Ethics **4**, 51–54 (2000)
31. Poullet, Y., Rouvroy, A.: Ethique et droits de l'homme dans la société de l'information, 13–14 septembre 2007. Strasbourg: Rapport général introductif, Council of Europe & UNESCO, Strasbourg (2007)
32. Prohansky, H., Fabian, A., Kaminoff, R.: Place identity, physical world, socialization of the self. J. Environ. Psychol. **3** (1983)
33. Rea, A.: L'avenir de l'Europe : l'immigration sans fin. Rev. Droits Etrangers **121** (2002)
34. Rey, A.: Dictionnaire historique de la langue française, éd. Le Robert (1992)
35. Rouvroy, A., Poullet, Y.: The right to informational self-determination and the value of self-development. Reassessing the value of privacy for democracy. In: Reinventing Data Protection. Actes de la conférence internationale des 12–13 octobre 2007, à paraître
36. Rouvroy, A., Poullet, Y.: Self-determination as the "key" concept. In: Reinventing Data Protection, International Conference co-organized by the University of Tilburg, the Information Technology & Law Research Centre, University of Namur, and the Vrij Universiteit Brussels, 12–13 October 2007 (2007)
37. Sasse, A.: Cybertrust and crime prevention: Usability and trust in information systems. In: Foresight Cybertrust and Crime Prevention Project, 04/1151, 10 juin 2004
38. Schmitt, C.: Théologie politique, 1922, rééd. Gallimard (1988)
39. Tugendhat, E.: Conférences sur l'éthique, Paris (1998)
40. Velu, J., Ergec, R.: La Convention européenne des droits de l'homme. Bruylant, Bruxelles, 1990, n^{o} 194
41. Wildt, A.: Menschenrechte und moralische Rechte. In: Gosepath, S., Lohmann, G. Philosophie der Menschenrechte, Francfort (1998)
42. Zamiatine, E.: Préface de Jorge Semprun. In: Nous Autres. Gallimard, Paris (1979)