LES ASPECTS JURIDIQUES DE LA BIOMETRIE par Claudine GUERRIER, avec la participation de Laure-Anne Cornelie

Selon le dictionnaire[1], la biométrie est « la science qui étudie, à l'aide des mathématiques, (statistiques, probabilités) les variations biologiques à l'intérieur d'un groupe déterminé ».
A la question « Qu'est-ce que la biométrie ? »[2], Actronix répond de façon plus pragmatique. Il part d'un constat : il existe trois moyens d'identification d'une personne : la possession (carte, badge, document), la connaissance (le mot de passe), ce qu'elle est, la biométrie. Ce constat conduit à une définition : « La biométrie permet l'identification d'une personne sur la base de caractères physiologiques ou de traits comportementaux automatiquement reconnaissables et vérifiables ». Il y a ici glissement progressif entre la science biométrique, qui a divers domaines d'application et la technique biométrique. D'une façon générale, le terme « biométrie » renvoie à la technique biométrique. Cette dernière connaît une expansion spectaculaire : de 47 millions d'euros en 1999, elle est passée à 600 millions d'euros[3] en 2003. L'étude du Gartner Group [4] insiste sur le développement de la biométrie (la technique biométrique) non seulement aux EUA, mais aussi dans la plupart des pays occidentaux. La science biométrique continue à connaître des heures heureuses. Beaucoup de chercheurs travaillent actuellement sur l'amélioration des techniques biométriques.
Il n'existe pas pour l'instant en Europe de définition juridique de la biométrie. Au Québec, la loi concernant le cadre juridique des technologies de l'information[5], dont l'objectif est d'assurer la sécurité juridique des communications effectuées au moyen de documents, l'équivalence fonctionnelle des documents et leur valeur juridique, consacre plusieurs paragraphes à la technique biométrique. La loi précise que nul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. En droit, la biométrie est donc un procédé d'identification appliqué aux personnes physiques[6].
L'industrie[7] classe les systèmes biométriques en deux catégories : la biométrie morphologique ou physiologique[8] et la biométrie comportementale[9]. La biométrie morphologique identifie les traits physiques spécifiques qui sont uniques, permanents pour chaque individu ; elle distingue la reconnaissance des empreintes digitales, de la forme de la main, de la forme du visage, de la rétine et de l'iris de l'œil.
La biométrie comportementale identifie certains comportements d'une personne physique comme le tracé de sa signature, l'empreinte de sa voix, sa démarche, sa façon de taper sur un clavier.
Les autorités de régulation, telles la CAI[10]au Québec et la CNIL [11]en France reprennent ces distinctions[12] auxquelles elles ont ajouté l'analyse de l'ADN, du sang et des odeurs. La

---

[1] Petit Robert, 2003
[2] www.actronix.fr
[3] Selon l'International Biometric Group
[4] Sur l'émergence des nouvelles technologies
[5] L.Q.2001,c.32, articles 44 et 45
[6] cf : supra : protection des données personnelles et protection de la vie privée.
[7] « La biométrie au Québec : les enjeux », document d'analyse, Commission d'accès à l'information, par Max Chassé
[8] en anglais : physiological
[9] en anglais : behavioral
[10] Commission d'accès à l'information
[11] Commission nationale de l'informatique et des libertés, autorité administrative indépendante.
[12] Cf : « les contrôles d'accès par biométrie », chapitre 4, 21eme rapport d'activité, CNIL, 2000

recherche débouche sur de nouveaux types biométriques, la forme de l'oreille et la thermographie faciale.
Les performances des systèmes biométriques n'atteignent jamais 100%. Pour l'instant, la perfection n'existe pas en biométrie.[13]
Afin de déterminer la performance des systèmes biométriques, deux mesures sont utilisées : le taux de faux rejets[14], qui exprime le pourcentage de personnes autorisées rejetées par le système, le taux de fausses acceptations[15], qui exprime le pourcentage de personnes non autorisées acceptées par le système.[16]
Les techniques biométriques existent depuis longtemps. Les empreintes digitales ont été exploitées dès le dix-neuvième siècle par l'institution policière. Au vingt-et-unième siècle, avec l'expansion de l'idéologie, de l'économie, du droit[17]sécuritaires, la biométrie devient un marché porteur. L'image de la biométrie est ambivalente. Adjointe à l'efficacité policière, elle est pourfendeuse de délits et de crimes, elle est le meilleur défenseur de la société civile[18]. Placée dans un contexte politique délétère, elle est le suppôt et le support des régimes totalitaires[19]. Dans « Le deuxième cercle »[20], l'utilisation de la reconnaissance vocale, avec un très fort taux de TFR et de TFA, brise des vies et devient un outil de répression au service de Staline.
L'essor exponentiel des procédés biométriques met en exergue les acteurs privilégiés que sont les chercheurs et les industriels.
Le droit n'est pas absent de la scène. Pour les chercheurs et pour les industriels, le droit représente une contrainte dont il faut tenir compte mais qu'il convient de minimiser. Pour les organisations de défense des droits de l'homme, la biométrie se doit d'être régulée par l'instrument législatif. Pour les tenants du commerce électronique, droit et biométrie ne sont pas antagonistes.
Deux thématiques affleurent : les libertés individuelles et la protection des données personnelles, d'une part, la signature électronique et la certification, d'autre part.
Dans une économie globalisée, certaines questions juridiques afférentes à la biométrie sont réglées au niveau international. Dans la plupart des cas, le droit de la biométrie s'impose au niveau des Etats et des régions[21]. Cela permet d'envisager une étude de droit comparé, à partir de la thématique esquissée ci-dessus et une certaine modélisation.

[13] « Il est impossible d'obtenir une coïncidence absolue (100% de similitude)entre le fichier signature créé lors de l'enrôlement et le fichier signature créé lors de la vérification » Les technologies biométriques, Performances des systèmes, Biométrie Online.
[14] TFR
[15] TFA
[16] Ce TFR et ce TFA font l'objet de campagnes marketing dans les milieux industriels.
[17] Patriot Act aux USA, RIPA au Royaume-Uni, loi sur la sécurité quotidienne, loi sur la sécurité intérieure en France. Supra.
[18] Romans policiers pour enfants et pour adultes
[19] Romans et films de science fiction
[20] Soljenitsyne
[21] cf : Union européenne

LA BIOMETRIE ET LE DROIT INTERNATIONAL

Le droit international n'existe pas pour l'instant, à proprement parler, en matière de biométrie. Il n'existe aucun équivalent de l'UIT.
Néanmoins, certains paramètres sont transnationaux et sont considérés comme tels. C'est ainsi que la maîtrise des flux migratoires préoccupe tous les pays occidentaux. Par ailleurs, la standardisation, bien difficile à mettre en place, conditionne la politique et le droit de la biométrie. La protection des données personnelles est prise en compte.

Le contrôle de flux migratoires est un souci pour tous les pays occidentaux où l'immigration est importante. L'identification des personnes physiques qui entrent sur le sol d'un Etat étranger n'est pas toujours évidente. Officiellement, vient s'ajouter la crainte d'une menace terroriste venue de l'étranger : ceci correspond à la position des EUA.
Le G8[22] a décidé, en mai 2003[23] de choisir le procédé biométrique le plus approprié. Un groupe d'experts est constitué pour proposer une solution appropriée. Cette procédure présente un certain caractère d'urgence puisque les EUA ont décidé d'exiger des étrangers des passeports utilisant les techniques biométriques. La France est plutôt favorable à l'utilisation des empreintes digitales. Cependant, d'autres choix sont possibles : l'Allemagne préfère la reconnaissance par l'iris,[24]les EUA utilisent surtout les empreintes digitales . D'ici peu de temps, les déplacements dans les Etats du G8 impliqueront le recours à des visas et des passeports biométriques. Cette solution est critiquée par certaines associations de défense des droits de l'homme qui mettent l'accent sur le danger d' atteinte aux libertés individuelles. En effet, la liberté de circulation, non seulement pour les marchandises[25], mais pour les personnes physiques, est un principe de base adopté et défendu par les démocraties. Les défenseurs des visas et des passeports biométriques arguent que l'identification biométrique n'est pas une atteinte portée à la liberté de circulation, mais simplement une mesure de maîtrise destinée à empêcher d'éventuels ennemis de la liberté de nuire aux pays démocratiques.
De son côté, l'OACI[26] recommande, puis impose[27]l'utilisation de la reconnaissance faciale.

Par ailleurs, la normalisation joue un rôle déterminant, dans le domaine de la biométrie, comme dans tous les autres domaines.
Des normes de compatibilité et d'interface ont été conçues pour faciliter l'usage des techniques biométriques. L'HAAPI[28] et le BAAPI[29] sont à la base d'un standard générique qui a été adopté le 13 février 2002. Le Common Biometric Exchange File Format[30] a en outre été adopté en janvier 2001. En 2002, l'OASIS[31] a initié un groupe de travail ayant pour finalité la définition des bases de description des données et des fonctions biométriques reposant sur le langage XML.

---

[22] Les sept pays les plus industrialisés, auxquels s'adjoint la Russie
[23] la réunion se tenait en France
[24] le procédé qui minimise les TFR et les TFA
[25] liberté commerciale
[26] ICAO, en anglais : International civil Aviation Organization
[27] En mars 2003
[28] Human Authentification Application Programmer Interface
[29] Biometric Authentification Application Programmer Interface
[30] CBEFF
[31] Organisation for Structured Information Standards

La standardisation a d'abord connu un essor aux EUA qui ont consenti un effort de recherche au niveau fédéral. En raison de l'enjeu sécuritaire, une collaboration a été instituée entre le Biometric Consortium et la NSA.
Au niveau international, c'est l'organisation internationale de normalisation[32] qui s'occupe de la standardisation. L'ISO se décompose en comités et le comité qui s'occupe de la biométrie est le JTC 1/ SC 37. Ce comité a pour finalité la normalisation des technologies non spécifiques du domaine de la biométrie, conçue pour faciliter l'interopérabilité et l'échange de données entre applications et systèmes. Parmi ces normes de biométrie non spécifiques, il convient de citer des formats de fichiers communs, des interfaces de programmation des applications, des modèles biométriques, des techniques de protection des modèles, des profils d'application et de mise en œuvre et des méthodologies appliquées à l'évaluation de la conformité.[33]
Un autre organisme s'intéresse à la biométrie : la Commission électrotechnique internationale.[34]De nombreux travaux sont réalisés au sein du sous-comité sur l'identification des cartes et des personnes du Comité technique mixte de l'ISO et de la CEI sur les technologies de l'information. Il s'agit de l'ISO/CEI JTC 1/SC 17
Depuis 1999, le SC 17 s'est penché sur des questions associées à la biométrie :

- l'utilisation des technologies qui permettent l'identification des personnes
- le stockage des données de biométrie dans des cartes d'identification à puce[35]
- l'adoption des normes autres que celles de l'ISO et de la CEI
- la connaissance des exigences particulières à certaines cartes et à certains systèmes de lecture de cartes.

Les groupes de travail du SC17 sont à l'origine de normes qui doivent assurer à tous les Etats un recours uniforme à la biométrie. Le groupe de travail sur les cartes d'identification [36], JTC 1/SC 17/WG3, considère que son objectif principal est d'améliorer la sécurité aux frontières grâce à un procédé adéquat d'identification des voyageurs. Les EUA, le Canada, l'Australie, la Nouvelle-Zélande, l'Allemagne, les Pays-Bas ont participé de manière particulièrement active à cette recherche de standardisation. Les experts du G8 ont pris en compte les tâches effectuées par ce groupe de travail sur les cartes d'identification. [37]
Un autre domaine de recherche dans le cadre du SC17 est celui des permis de conduire internationaux[38]. Certaines personnes morales, notamment les Nations Unies, redoutent que le permis actuel soit facile à falsifier. En conséquence, le groupe de travail sur les permis de conduire pour véhicule à moteur et documents associés du SC 17/ WG 10 concocte des lignes directrices pour la conception de cartes lisibles par machine. Les travaux de normalisation vont connaître des développements importants dans les années à venir. Dans chaque Etat, une entité est le correspondant des organismes internationaux de standardisation. Par exemple, au Canada, c'est le Conseil canadien des Normes qui collabore avec l'ISO et le CEI.[39]

---

[32] ISO, en anglais. Cf : www.iso.ch

[33] La première réunion du JTC 1/SC 37 se tient du 11 au 13 décembre 2003 en Floride
[34] CEI
[35] « cartes intelligentes »
[36] Documents de voyage lisibles par machine
[37] « Le groupe de travail a participé à toutes les discussions portant sur les technologies associées à la biométrie, a précisé M.Shaw . Les gouvernements ont établi des exigences. C'est au groupe de travail de l'ISO/CEI d'y répondre ». www.scc.ca/ « La sécurité sous un jour nouveau grâce à la biométrie , le Conseil canadien des normes »

[38] IDP
[39] CCN

Au Japon, un consortium regroupe trois ministères : Ministry of Economy and Industry, Ministry of Land Infrastructure and Transport, le Gaimusho (ministère des affaires étrangères) et une vingtaine d'entreprises japonaises dont Hitachi, Mistsubishi, KDD. L'objectif est d'unifier les normes et les technologies utilisées en biométrie .
En France, l'organisme spécialisé dans la normalisation et qui coopère notamment avec l'ISO est l'AFNOR (Agence française de normalisation). L'AFNOR a créé un comité de normalisation FTS [40] au sein de la Commission générale CG CSA[41]. Ce comité de normalisation FTS est chargé d'étudier cinq secteurs en conjonction avec les cartes d'identification : biométrie, et aussi signature électronique, protocoles sécurisés sur réseaux ouverts. Les travaux ont commencé en mars 2002 et ont continué à se développer en 2003. Une nouvelle commission AFNOR sur la biométrie CN37 est instituée en janvier 2004. Deux groupes de travail ont été créés : GT1 : Techniques biométriques, GT2 : profils d'utilisation de la biométrie.
Le rapport Cabal, déposé sur le bureau de l'Assemblée nationale à la mi-juin 2003[42], met l'accent sur l'intérêt de la normalisation. Le contexte est très mouvant : les techniques biométriques sont largement propriétaires et dispersées. La normalisation, qui revêt des aspects juridiques, traduit les rapports de force industriels au-delà des frontières. Les industriels français ne sont pas en mauvaise position [43]. Les négociations à venir dans le domaine de la normalisation mettront en exergue les vainqueurs de la standardisation internationale dans le domaine de la biométrie.

Enfin, la protection des données personnelles joue un rôle déterminant en matière de biométrie. L'OCDE[44] adopte les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel. Ces lignes directrices, qui revêtent la forme d'une recommandation du conseil de l'OCDE, ont été initiées par un groupe d'experts gouvernementaux, sous la présidence de M.D.Kirby[45]. Elles ont pris effet le 23 septembre 1980. Elles traduisent un accord sur les principes qui seront développés dans les législations nationales. Elles interdisent le stockage illicite de données à caractère personnel, l'utilisation abusive ou la divulgation non autorisée de ces données. Un certain nombre de pays se sont inspirés des lignes directrices de l'OCDE.
En outre, les représentants des Etats qui ont adopté des lois sur la protection des données personnelles se réunissent chaque année lors des conférences des commissaires à la protection des données. A l'occasion de la XXIII ème[46]conférence internationale des commissaires à la protection des données, un débat a été organisé sur les usages et sur l'opportunité de la biométrie, soupçonnée d'être potentiellement liberticide. Ils ont émis des réserves particulières face à la technique de reconnaissance des visages, destinée à prévenir la délinquance et la criminalité. Cette technique a notamment été expérimentée au Royaume-Uni, soumis au droit de l'Union européenne en matière de protection des données personnelles. A Newham, la ville a été équipée d'un CCTV, système de vidéosurveillance en circuit fermé couplé à une technologie qui permet d'alerter la police si une personne dont l'image est présente dans les fichiers de la police se présente. Pour sauvegarder la vie privée et l'intimité, les experts des Data Protection Registrars ont émis une recommandation visant à mettre en place une autorégulation, un code de bonne conduite. Il n'y aurait plus

[40] Fonctions transverses et Systèmes
[41] Cartes et systèmes associés.
[42] Cf : supra
[43] « … nous devons participer à la normalisation des méthodes de biométrie afin que les procédés retenus correspondent aux systèmes proposés par nos entreprises » explique le député Cabal. In news.zdnet.fr. juin 2003
[44] Organisation de coopération et développement économique
[45] Alors Président de la Commission australienne de la réforme législative.
[46] La conférence s'est tenue du 24 au 26 septembre 2001

d’interférence dans la vie privée, comme l’exige la loi. Les visages scannés ne sont sauvegardés que s’ils correspondent à une personne fichée dans la base de données. Le taux d’erreurs ne peut être évalué, mais il ne semble pas négligeable. De plus, le système de sauvegarde de la vie privée semble insuffisant. L’ONG britannique Privacy international considère que la reconnaissance faciale publique ou semi-publique est à proscrire. La XXIIIème conférence internationale des commissaires à la protection des données s’est finalement prononcée contre la reconnaissance faciale.

VIE PRIVEE ET PROTECTION DES DONNEES PERSONNELLES

La principale problématique en matière de biométrie concerne les libertés individuelles et la protection des données personnelles. Les industriels souhaitent que les contraintes juridiques en la matière soient réduites au minimum. Ils insistent sur un progrès induit par la biométrie : l’impossibilité de procéder à une usurpation d’identité. Le discours explicite et implicite des

acteurs qui optent pour une minimisation des contraintes juridiques insiste sur la sécurité à laquelle concourt grandement la biométrie.
A l'inverse, les défenseurs des droits de l'homme insistent sur les dangers que génère la biométrie en matière de libertés individuelles, de protection de la vie privée, de la protection des données personnelles.
Ces deux discours sont légitimes.
La sécurité est prise en compte dans les technologies de l'information depuis le début du vingt-et-unième siècle.
La Convention du Conseil de l'Europe sur la cybercriminalité[47] annonce son intention de lutter contre les atteintes au système informatique[48], contre la pédopornographie, la contrefaçon ; une entraide entre polices[49]est instituée au niveau des Etats[50].
Les Etats-nations sont, de façon concomitante, à l'origine de textes destinés à combattre les délits et les crimes dans la société de l'information.
Ainsi, le Patriot Act[51] est-il adopté le 24 octobre 2001. Cette loi permet au FBI de brancher le système Carnivore sur le réseau d'un fournisseur d'accès à Internet et de surveiller les traces de navigation sur le web d'une personne suspectée d'être en rapport avec un présumé terroriste. Il assouplit aussi les procédures jusque là nécessaires pour procéder à des interceptions de télécommunications[52].
Au Royaume-Uni, le RIPA permet de conserver des données de connexion.
En France, la loi relative à la sécurité quotidienne[53] autorise la conservation, pendant un an, de données afférentes à une communication[54]. Elle exige la remise au clair, à la demande du Procureur de la République, du juge d'instruction, des conventions de cryptologie. La loi sur la sécurité intérieure[55] précise que les fournisseurs d'accès à Internet doivent mettre à la disposition d'un officier de police judiciaire les informations nécessaires à la manifestation de la vérité.
Ces textes ne sont pas relatifs à la biométrie mais ils introduisent un corpus juridique qui fonde dans chaque Etat les bases de l'influence sécuritaire dans la société de l'information. Dans chacun de ces Etats, les lois ont été votés à l'unanimité ou à la quasi unanimité par les différents partis. Une opposition ne s'est guère fait entendre. L'Exécutif et le Législatif sont en parfaite harmonie. La société civile elle-même semble adhérer à ces dispositions sécuritaires.
Un difficile équilibre a été recherché, depuis une vingtaine d'années, entre le souci de sécurité et l'attachement aux libertés individuelles, à la protection de la vie privée. Il semble que l'équilibre penche actuellement en faveur de la sécurité.
Néanmoins, le droit à la vie privé, le respect du corps humain font partie des acquis juridiques que la plupart des Etats reconnaissent.
La biométrie peut poser problème face à l'inviolabilité du corps humain. En effet, la plupart des techniques biométriques impliquent la mise en jeu du corps humain.

---

[47] Convention du 23 novembre 2001, signée par les Etats-membres du Conseil de l'Europe, les USA, le Canada, le Japon, l'Afrique du Sud, non encore ratifiée.
[48] En France, délit depuis l'adoption de la loi Godfrain en 1988
[49] Et non une cyberpolice, comme l'auraient souhaité les USA
[50] Le travail d'Interpol demeure indispensable
[51] Provide Appropriate Tools Required to Intercept and Obstruct Terrorism
[52] Il était nécessaire d'avoir l'agrément de l'Attorney general (le ministre de la justice), et d'obtenir l'accord d'une FISA Court
[53] loi du 15 novembre 2001
[54] « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales (article 29 de la LSQ)
[55] Définitivement adoptée le 13 février 2003

Le respect du corps humain est un héritage des religions monothéistes, qui ont joué un rôle important dans l'édification des normes et des lois. L'homme, l'être humain aurait été créé à l'image de Dieu. C'est pourquoi le corps vivant ou même mort[56] est honoré. Au vingt-et-unième siècle, la plupart des sociétés sont laïques, mais le corps humain est protégé par la loi.
En France, tout commerce en relation avec le corps humain est prohibé.[57]La loi du 29 juillet 1994[58] est intervenue pour empêcher une dérive génétique. Des éléments traditionnels sont repris : inviolabilité, incompatibilité entre le corps humain et les droits patrimoniaux[59], intégrité du corps humain[60]. Des thèmes nouveaux interviennent : interdiction de l'eugénisme[61], prohibition des mères porteuses[62].
La reconnaissance faciale ne nécessite pas le consentement des intéressés. Il peut en être de même pour les empreintes digitales. Est-il légitime de capter des éléments en relation avec le corps humain sans l'accord des personnes ? Les réponses ne sont pas unanimes.
De plus, il peut y avoir rapprochement entre biométrie et vie privée : certaines techniques biométriques sont susceptibles de renseigner autrui sur la santé des personnes concernées[63].
Le droit à la vie privée, quant à lui, est reconnu par les instances internationales. Au niveau des instances onusiennes, la déclaration universelle des droits de l'homme détient une haute valeur symbolique : « Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes »[64]. Près de vingt ans plus tard, des principes identiques sont repris dans le Pacte international relatif aux droits civils et politiques[65].
Le Conseil de l'Europe met en exergue la vie privée dans la Convention européenne des droits de l'homme.[66]Dans les Etats qui ont ratifié la Convention européenne de sauvegarde des droits de l'homme et le droit de requête individuelle, les citoyens, après avoir épuisé les voies de recours interne, sont en droit de saisir la Cour européenne des droits de l'homme. Un Etat condamné pour violation de la vie privée, doit non seulement indemniser la victime, mais aussi modifier les lois qui sont à l'origine du dysfonctionnement juridique.
La Charte européenne des droits de l'homme[67] envisage les différents droits de l'homme, y compris les droits sociaux. Elle englobe le droit à la vie privée. Elle se voit reconnaître valeur constitutionnelle.
En France, le Code Civil[68]reconnaît aussi le droit à la vie privée.[69]

---

[56] La plupart des Etats sont intervenus sur le devenir du corps humain après la mort. Dans les pays majoritairement chrétiens et musulmans, la crémation a longtemps été interdite. Les sépultures étaient régies par une règle écrite ou par la coutume.
[57] Les ventes de sang sont interdites.
[58] Loi n° 94653 du 29 juillet 1994
[59] Article 16-5 du Code Civil : « Les conventions ayant pour effet de conférer une valeur patrimoniale au corps humain, à ses éléments ou à ses produits sont nulles »
[60] Article 16-3 du Code Civil : « Il ne peut être porté atteinte à l'intégrité du corps humain qu'en cas de nécessité médicale pour la personne. Le consentement de l'intéressé doit être recueilli préalablement hors le cas où son état rend nécessaire une intervention thérapeutique à laquelle il n'est pas à même de consentir »
[61] Article 16-4 du Code Civil : « Toute pratique eugénique tendant à l'organisation de la sélection des personnes est interdite. Sans préjudice des recherches tendant à la prévention et au traitement des maladies génétiques, aucune transformation ne peut être apportée aux caractères génétiques dans le but de modifier la descendance de la personne »
[62] « Toute convention portant sur la procréation ou la gestation pour le compte d'autrui est nulle »
[63] cf : infra.
[64] Article 12 de la Déclaration universelle des droits de l'homme
[65] Article 17 « Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et sa réputation »
[66] Article huit de la Convention européenne de sauvegarde des droits de l'homme.
[67] Décembre 2000

Parce qu'il y a droit à la vie privée, il y a aussi protection des données personnelles, protection des données nominatives informatisées. Néanmoins, les normes ne sont pas identiques dans les différents Etats. C'est pourquoi cette étude sur la biométrie est d'abord une étude comparative. Si la biométrie est avant tout transnationale, une modélisation s'impose selon les régions et la culture juridique.
Dans chaque région, les mêmes questions s'imposent : la biométrie assure-t-elle correctement la sécurité en matière de demandes d'asiles, de visas, de passeports, de cartes d'identité ?
Comment prendre en compte les culture nationales ? Comment aborder les diverses applications : accès à des zones sécurisées, accès à des zones non sécurisées, accès à l'entreprise et contrôle des horaires ?

LA BIOMETRIE ET LA PROTECTION DES DONNEES PERSONNELLES

PREMIER MODELE : UNION EUROPEENNE ET QUEBEC

L'Union européenne et le Québec sont très protecteurs en matière de protection des données personnelles. Les industriels doivent donc supporter certaines contraintes dans le domaine de la biométrie.
Au sein de l'Union européenne, les directives européennes sur la protection des données personnelles[70], notamment dans le secteur des télécommunications, puis des communications électroniques[71] ont pour fil conducteur le respect de la vie privée. La directive de 1995 s'applique aux personnes physiques identifiées ou identifiables[72]. La personne identifiable peut être reconnue par des éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. Si le terme « biométrie » n'apparaît pas dans le texte, il est visé, sans aucun doute, par la directive. En effet, les usages biométriques sont en relation étroite, constante, avec l'identité physique et physiologique des personnes. Les fournisseurs de biométrie sont tenus de se conformer à la directive européenne, s'ils ont leur siège ou un établissement dans un pays de l'Union européenne. Les applications « domestiques » ne sont pas concernées mais dès qu'une banque de données biométrique est constituée, la directive de 1995 s'applique. Cela implique de nombreuses contraintes, dans le domaine des données sensibles, du profil, du jugement ou de la décision arrêtés uniquement sur la base de données nominatives. Des procédés biométriques peuvent être considérés comme inconciliables avec la directive de 1995[73]. Le recours à certaines applications biométriques peut présenter un caractère excessif et disproportionné par rapport à la finalité du traitement.[74]
Le Québec, bien qu'état francophone membre d'une fédération de provinces américaines, le Canada, est très proche, sur le plan juridique, de l'Union européenne, et, en particulier, de la

---

[68] Article neuf
[69] La France a ratifié la Convention européenne de sauvegarde des droits de l'homme en 1974, le droit de requête individuelle en 1981.
[70] 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.
[71] La directive 97/66/CE du parlement européen et du Conseil du 15 décembre 1997 est afférente au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des télécommunications. Elle est abrogée après l'entrée en vigueur de la directive du 12 juillet 2002 sur la protection des données personnelles dans le secteur des communications électroniques.
[72] Article deux de la directive 95/46/CE : définition des « données à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable
[73] Bien que cela ne se soit pas produit pour l'instant
[74] L'article six de la directive stipule « les données à caractère personnel doivent être…adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ultérieurement »

France. L'influence du Code civil napoléonien se fait sentir. Le Québec, en matière de protection des données nominatives informatisées, a même devancé l'Union européenne. Ses lois trouvent leur origine dans la Charte des droits et libertés de la personne, de 1975. La loi sur la protection des renseignements personnels dans le secteur privé fut adoptée en 1994[75].Cette loi québécoise, au même titre que la directive de 1995, régit la collecte, la conservation, l'utilisation et la communication des données. Elle admet le droit d'accès et de rectification. C'est la Commission d'accès à l'information qui se voit confier le soin de trancher les litiges. Une autre loi est afférente au secteur public : la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.[76]
En 2001, des mesures législatives sur les techniques biométriques ont été prises dans le cadre de la loi concernant le cadre juridique des technologies de l'information. Sur ce point, le Québec est en avance sur l'Union européenne et se montre protecteur au regard de la vie privée.[77]L'institution[78] d'une banque de caractéristiques ou de mesures biométriques doit être préalablement divulguée à la Commission d'accès à l'information.

Si le contrôle des flux migratoires est conciliable avec la directive de 1995, les applications des techniques biométriques posent question aux autorités de régulation, et le principe de subsidiarité permet d'observer une certaine variabilité dans les cultures juridiques nationales.

I/ **La maîtrise des flux migratoires grâce à la biométrie, l'utilisation de la biométrie pour les visas, les passeports, sont considérées comme compatibles avec la directive de 1995.**
Le principe de la libre circulation des personnes est mentionné dans le traité de Rome, de même que la libre circulation des marchandises. Le traité d'Amsterdam pose les bases de cette libre circulation. Il reprend les accords de Schengen, initialisés en 1985 et entrés en vigueur en 1995
Les personnes étrangères à l'Union européenne peuvent demander le droit d'asile aux pays de l'Union européenne qui sont des démocraties et qui doivent protéger les personnes persécutées dans leur Etat d'origine.
Il n'en demeure pas moins que l'Union européenne veut rester maîtresse de ses flux migratoires[79]
A/ Cette maîtrise des flux migratoires est conciliable avec la directive de 1995
1) La Convention de Dublin et surtout son application prennent en compte la directive-cadre relative à la protection des données personnelles.

La Convention de Dublin[80], applicable à partir de 1997 et à laquelle tous les Etats-membres de l'Union européenne sont parties traite des demandes d'asile et du contrôle des demandes d'asile. Il s'agit d'éviter l'entrée irrégulière d'étrangers sur le territoire de l'Union européenne. En raison des fraudes possibles, les ministres en charge de l'immigration

[75] « Une personne qui exploite une entreprise au Québec et qui transmet des renseignements à l'extérieur de nos frontières et qui transmet des renseignements à l'extérieur de nos frontières relativement à un résident québécois doit prendre tous les moyens raisonnables pour qu'ils soient aussi bien protégés que s'ils étaient conservés ou utilisés ici » a déclaré André Ouimet, qui fut secrétaire de la Commission d'accès à l'information.
[76] L. R. Q., c A-2.1, loi sur l'accès
[77] Articles 44 et 45.
Article 44 : « Nul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. L'identité de la personne ne peut alors être établie qu'en faisant appel au minimum de caractéristiques ou de mesures permettant de la relier à l'action qu'elle pose et que parmi celles qui ne peuvent être saisies sans qu'elle en ait connaissance.
[78] Article 45
[79] Notamment en matière de migrations économiques.
[80] Convention du 15 juin 1990, complétée par le règlement n°343/2003 du Conseil du 18 février 2003

établissent, à l'échelle européenne, un projet visant à comparer les empreintes digitales des demandeurs d'asile.

2) Avec l'entrée en vigueur du Traité d'Amsterdam, un nouveau fondement juridique quant à la politique de demande d'asile est envisagé. C'est le règlement du 11 décembre 2000[81] qui est adopté par le Conseil et le Parlement. Ce règlement permet de stocker les empreintes digitales des demandeurs d'asile. Le choix de la Commission s'est porté sur les empreintes digitales. En effet, c'est la technique biométrique la plus utilisée en Europe. De plus, c'est une technique assez sûre[82]. Le débat devant le Parlement , au regard de la protection des libertés individuelles, est assez vif. Par deux avis en date des 7 juillet et 21 septembre 2000, le Parlement s'était opposé à l'enregistrement des empreintes digitales des mineurs. Le Conseil a passé outre.[83] Les données enregistrées sont les empreintes digitales, l'Etat d'où le demandeur d'asile est originaire, le sexe, le numéro de référence. Elles sont conservées pendant dix ans (sauf si le demandeur d'asile obtient la citoyenneté d'un pays de l'Union européenne) et sont codées. La protection des données personnelles n'est pas occultée. L'utilisation, la transmission, la conservation, l'effacement des données sont conformes à la directive de 1995. La Commission veille particulièrement à la sécurité des données.[84]Elle informe le Parlement et le Conseil des mesures prises par ses soins. Tout demandeur d'asile victime d'un préjudice en raison d'une mauvaise application du règlement percevra une compensation. L'Etat concerné sera exempté, partiellement ou entièrement, de sa responsabilité, s'il démontre qu'il n'est pas partie prenante dans l'événement à l'origine des dommages. Une autorité de contrôle indépendante commune est instituée : elle est composée de deux représentants des organismes de régulation de chaque Etat-membre.

Un autre règlement, destiné à la mise en application du précédent règlement est adopté par le Conseil et le Parlement[85]. Il explicite certaines caractéristiques d'Eurodac.

B) Eurodac est entré en vigueur dans l'Union européenne le 15 janvier 2003. Il comprend un système central d'identification des empreintes digitales des demandeurs d'asile[86]et dans seize pays européens un système de transmission électronique des empreintes digitales dont l'objectif est de lutter contre l'immigration clandestine. En effet, avec Eurodac, les Etats-membres peuvent identifier les demandeurs d'asile et les personnes qui franchissent irrégulièrement une frontière extérieure de la Communauté. Après comparaison des empreintes, les Etats sont susceptibles de savoir si un demandeur d'asile ou un ressortissant étranger en situation illégale a déjà formulé une demande dans un autre Etat de l'Union européenne. La finalité est de combattre les demandes d'asile multiples.

   L'unité centrale de comparaison d'empreintes digitales appelée AFIS[87]est gérée par la Commission européenne. La base de données informatisée, les moyens électroniques de

---

[81] Règlement n° 2725/2000 du Conseil du 11 décembre 2000 ; parution au Journal Officiel de l'Union européenne le 15 décembre 2000.

[82] « Nous prenons des empreintes des dix doigts, ce qui permet d'arriver à un taux d'erreur de seulement 0 ?1%. La technologie rétinienne est peut-être encore un peu plus sûre mais elle est plus chère, et qui plus est aux mains d'un seul fabricant, ce qui nous gêne. Et surtout : elle n'a jamais été déployée à grande échelle » a déclaré Frank Paul, chef de l'unité projets informatiques à grande échelle de la Commission européenne, dans Jdnet solutions. 5 février 2003.

[83] En France, le Groupe d'information et de soutien des immigrés (GISTI) s'étonne que le Parlement n'ai pas été suivi. Il est vrai que le GISTI s'oppose en permanence au fichage des personnes en situation irrégulière.

[84] Cf : article 17 de la directive de 1995. Article 4 de la directive du 12 juillet 2002. Alinéa 2 : « Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, le fournisseur d'un service de communications électroniques accessible au public informe les abonnés de ce risque et, si les mesures que peut prendre le fournisseur du service ne permettent pas de l'écarter, de tout moyen éventuel d'y remédier, y compris en indiquant le coût probable ».

[85] Règlement 407/ 2002

[86] Sis à Bruxelles

[87] Automated Fingerprint Identification System

transmission sécurisée entre les Etats et la base de données centrale complètent Eurodac. L'unité centrale détermine les impératifs techniques nécessaires à la transmission des empreintes digitales par voie électronique. Si des problèmes techniques surviennent, il sera fait recours à d'autres moyens de transmission[88]. Le numéro de référence relie l'empreinte digitale à une personne physique, identifie l'Etat-membre qui a envoyé les données.

Eurodac a d'abord été testé au Royaume-Uni. Les étrangers demandeurs d'asile politique ont expérimenté des cartes à puce qui contenaient leurs empreintes digitales fournies par le ministère de l'Intérieur.[89]Une carte d'identité ARC[90]est remise au demandeur d'asile ; elle comprend les empreintes digitales, une photo, le nom patronymique, la date de naissance, la nationalité d'origine. Elle se substitue au formulaire antérieurement fourni sur support-papier, trop facilement falsifiable, selon les autorités.[91]

Avant l'instauration d'Eurodac, il était quasiment impossible de déterminer si un demandeur d'asile n'avait pas déjà déposé une demande dans un autre Etat signataire de la Convention de Dublin. Afin que la Convention soit applicable, il convenait de concevoir un système permettant à chaque Etat de contrôler si un demandeur d'asile a introduit préalablement une requête dans un autre Etat lié par la Convention.

Ces dispositions, depuis l'adoption des règlements et d'Eurodac s'appliquent à toute personne âgée de quatorze ans (ou plus), puisque les avis négatifs du Parlement européen n'ont pas été retenus.

Elles concernent les Etats de l'Union européenne, et trois Etats tiers qui se sont engagés à introduire Eurodac sur leur territoire : la Norvège, l'Islande, la Suisse. La biométrie, via les empreintes digitales, est donc généralisée dans la politique d'asile.

Par exemple, la Suisse, dès Octobre 2002, introduit le système FIT[92] dans les vingt-six polices cantonales suisses, reliées au système central de Berne. FIT, après l'AFIS, est une solution technique qui permet à chaque pays de se connecter à Eurodac. Il a le mérite de la compatibilité avec des standards internationaux[93]. Introduit d'abord en Norvège, il a plus de dix ans d'expérience en Scandinavie. Par ailleurs, le serveur NAP[94]achemine de manière sécurisée les communications sur le réseau Testa afférent aux administrations européennes. FIT a également été utilisé dans le cadre des accords de Schengen pour l'échange d'informations dans le réseau SIRENE[95]. Il permet aux polices d'échanger électroniquement des empreintes digitales et des photographies afin de parvenir à l'identification de personnes recherchées[96].

Eurodac respecte la directive de 1995 sur la protection des données personnelles. Le législateur européen a veillé à la prise en compte de cette exigence. Il est cependant critiqué par presque toutes les associations de droits de l'homme pour son caractère

---

[88] CDROM, disquettes, papier. Cf : règlement 407/2002 du Conseil

[89] Home Office

[90] Application Registration Card ; chaque carte ARC permet une vérification de l'identité d'un demandeur et compare les données biométriques codées sur la puce avec celles acquises auprès du requérant lors de sa demande.

[91] « Avec cette carte, le gouvernement fait usage de la pointe de la technologie pour lutter contre les fraudeurs, permettant de pouvoir identifier rapidement les demandeurs d'asile à chaque étape de leur demande » selon le ministre délégué à l'immigration, Jeff Rooker

[92] Fingerprint Image Transmission

[93] notamment Interpol et le FBI

[94] National Access Point

[95] Supplément d'Information Requis à l'Entrée Nationale

[96] « Le système FIT est le premier à pouvoir vérifier électroniquement et de manière hautement sécurisée des empreintes digitales. D'autre part, il correspond aux besoins des services de l'immigration nationaux de pouvoir identifier rapidement des empreintes digitales, lorsqu'ils détiennent des suspects pour des périodes courte durée.

xénophobe. L'usage des empreintes digitales ne s'en inscrit pas moins dans une tradition de travail policier et de contrôle des flux migratoires.

C) A l'occasion du Conseil de l'Union européenne de Salonique de Juin 2003[97], les chefs d'Etats et de gouvernement ont décidé l'introduction, pour 2005, de données biométriques : empreintes digitales, iris, ADN[98], dans les passeports et les visas.
La Commission européenne est déjà en charge d'une étude relative au développement d'un système d'information sur les visas[99]. Elle préconise de retenir deux éléments biométriques pour identifier les personnes et pour mieux sécuriser les titres de séjour et les visas. Le choix s'est porté sur la reconnaissance faciale, qui devra être numérisée et stockée sur carte à puce, insérée dans les documents d'identification, et sur l'empreinte digitale. L'Union européenne adopte une démarche proche des lignes directrices américaines.[100] Cette position est critiquée par les organismes de défense des droits de l'homme et par des organisations non gouvernementales.[101]Les Exécutifs sont fermement décidés à sécuriser les passeports et les visas. C'est pourquoi un projet européen de passeports biométriques est en train de se mettre en place : les passeports seront dotés, d'ici 2005, d'une puce où seront stockées les empreintes digitales ou les empreintes rétiniennes du titulaire. Les informations seront conservées sur le système d'information Schengen[102](SIS II prévu pour 2006) qui peut être consulté par des fonctionnaires dans toute l'Union européenne. En France, la loi de 2003[103]relative à la maîtrise de l'immigration et au séjour des étrangers en France prévoit la création d'un fichier recensant les empreintes digitales des personnes qui déposent une demande d'asile ou veulent obtenir un visa en France.

II/ Si les applications biométriques ont facilement pour finalité la sécurité, d'autres objectifs prêtent à controverse.

A) Lorsque la finalité est sécuritaire, les applications biométriques sont facilement acceptées par les autorités de régulation en matière de protection des données personnelles. La plupart des exemples seront empruntés au cas français

1) La CNIL admet la proportionnalité quand le site accueille des matières dangereuses. La CNIL[104] a émis un avis favorable à la suite d'une demande formulée par l'établissement de la Hague de la Cogema- Compagnie générale des matières nucléaires- tendant à installer un lecteur d'empreintes digitales à l'attention du personnel et des visiteurs[105]. En effet, le stockage de matières nucléaires n'est pas inoffensif et doit être contrôlé. Certaines Zones sont sous secret défense. L'institution d'une banque de données d'empreintes digitales se justifie.

---

[97] Il s'est tenu les 19 et 20 juin 2003
[98] Ce qui est relativement nouveau
[99] VIS
[100] Loi sur le renforcement de la sécurité aux frontières et sur la réforme des visas (« Enhanced Border Security and Visa Reform Act ») de mai 2002
[101] Par exemple, l'organisation Statewatch, ONG basée à Londres manifeste son opposition « La décision, par le Conseil européen, d'instaurer la surveillance généralisée des déplacements des personnes, a été prise sans aucune consultation publique ni aucun débat au Parlement » selon Tony Bunyan, le directeur de Statewatch. Ce dernier déclare aussi « Ces propositions ne sont qu'une autre conséquence de la guerre contre le terrorisme qui montre que l'Union européenne tient tout autant que les Etats-Unis à mettre en place des systèmes de surveillance massive, ayant plus à voir avec un contrôle politique et social qu'avec la lutte contre le terrorisme » au sujet des propositions de la Commission européenne.
[102] SIS II
[103] Loi n°2003.1119 du 26 novembre 2003
[104] Commission nationale de l'informatique et des libertés.
[105] Les dates et les heures d'entrées et de sorties sont enregistrées et conservées pendant un an pour les membres du personnel et deux ans pour les visiteurs.

2) La CNIL admet la proportionnalité quand le site est sensible pour des raisons diverses.
2.1) C'est le cas pour les aéroports de l'ensemble de l'Union européenne[106]. Les aéroports reçoivent un vaste public et il convient d'éviter d'éventuels actes de terrorisme.
2.1.1) Cela peut concerner certains vols.
Air France a testé, avec l'accord de la CNIL, une technique biométrique utilisant les empreintes digitales au départ de vols à destination de Tel-Aviv[107]. Il convient de s'assurer que le client d'Air France ayant déjà fait enregistrer un bagage est bien la personne qui embarque dans l'avion. L'empreinte digitale est relevée par le biais d'un boîtier électronique installé sur le comptoir d'enregistrement, puis comparée avec un boîtier similaire au moment de l'accès à bord. La CNIL, dans son avis favorable, a exigé le respect de la confidentialité des informations.
Au Royaume-Uni, un contrôle automatisé de passeports a été testé en partance de Madrid pour Londres-Heathrow et de Miami pour Standed[108]
2.1.2) Cela peut concerner certaines zones des aéroports.
A Roissy et à Orly, a été expérimenté un contrôle des « zones réservées sûreté [109]» : cela affecte l'accès des personnels des Aéroports de Paris, des services publics et des entreprises qui interviennent dans les zones dénommées « zones réservées sûreté ». Cette expérimentation utilise soit les empreintes digitales, soit la reconnaissance palmaire, soit l'iris. Elle est prévue pour une durée de six mois, et basée sur le volontariat. La CNIL a rendu un avis favorable[110], assorti de conditions. L'exigence sécuritaire respecte le principe de proportionnalité, mais le détournement de finalité doit être évité. Un bilan est effectué à la fin de l'expérimentation. Pendant l'expérimentation, le stockage a leu sur une base de données centralisée. A terme, est prévu un stockage sur carte à puce. Les trois applications de l'empreinte digitale, de la reconnaissance palmaire, sur l'iris sont possibles. Toutefois, c'est, en France, l'empreinte digitale qui est le plus fréquemment utilisée pendant la phase d'expérimentation. Les leçons tirées aux aéroports de Roissy et d'Orly sont riches d'enseignements, tant pour les industriels, qui souhaitent recourir à la biométrie que pour la CNIL, pour qui le recours à la biométrie doit revêtir un caractère exceptionnel. L'usage de la biométrie sera généralisé avant la fin 2003 pour le contrôle des personnels travaillant en zone réservée, puis étendu aux passagers.
2.2) Cela concerne aussi les services publics, dans les secteurs de l'éducation et de la culture.
2.2.1) La proportionnalité a été admise, partiellement, dans le cas de l'Académie de Lille, pour assurer la sécurité des concours. L'Académie de Lille a saisi la CNIL d'une demande d'avis afférente à l'accès du personnel de l'Education nationale dans les locaux académiques. Elle proposait un système de contrôle d'accès avec empreintes digitales et ne cherchait pas à contrôler le temps de présence du personnel. Les représentants du personnel ont été informés du projet ; le personnel, dans son ensemble, fait l'objet d'une campagne de communication ; selon le secrétaire général de l'Académie, il n'a manifesté aucune réaction de rejet.

---

[106] Cf : aéroport d'Amsterdam, qui utilise la technique de l'iris
[107] « Par cette expérimentation, Air France manifeste sa volonté d'innover et d'acquérir un leadership dans l'utilisation de nouvelles technologies permettant l'amélioration du traitement au sol de ses clients. Nous travaillons d'ores et déjà avec les autorités pour une utilisation générale de la biométrie » a déclaré en décembre 2002 Pascal de Izaguirre, directeur général adjoint Exploitation Sol de la compagnie. Air France est enthousiaste à l'égard de la biométrie, considérée comme une panacée.
[108] Avec, dans le premier cas, la collaboration de la compagnie Virgin Atlantic, dans le deuxième cas, la collaboration d'easyJet
[109] ZRS
[110] Délibération 02-034 du 23 avril 2002

La CNIL établit deux finalités : la première correspond à l'identification du personnel pouvant pénétrer dans les locaux académiques. La seconde met l'accent sur la sécurité des examens et des concours[111] qui sont organisés dans l'Académie et sur le statut du personnel habilité à accéder aux bâtiments en vue de l'organisation et de la surveillance des examens et des concours.

La première finalité, d'après la CNIL, ne justifie pas, en vertu du principe de proportionnalité, la constitution d'une base de données avec empreintes digitales. La seconde, au contraire, justifie la création d'une base de données avec empreintes digitales, sous réserve que les locaux concernés soient identifiés[112] : le concept de proportionnalité s'applique. La base de données est constituée de trois modules, le module « personne » avec les noms, prénoms et les identifiants permettant de saisir d'autres modules, le module « droit d'accès » avec les profils d'habilitation des personnes, le module « empreintes » avec les gabarits des empreintes digitales.

2.2.2) Biométrie et patrimoine culturel :

Le patrimoine culturel a besoin d'être sauvegardé et protégé pour des raisons différentes des aéroports, mais tout aussi valables. Les œuvres d'art ont une grande valeur financière, culturelle et, dans un musée, elles sont mises à la disposition du public.

En 2001, le musée du Louvre a déposé une demande d'avis afférent à l'utilisation de procédés biométriques pour assurer la sécurité des biens du musée et contrôler les heures de travail de salariés d'entreprises sous-traitantes chargées du nettoyage et de la maintenance.

Le musée du Louvre a agréé des contrats de sous-traitance, qui prévoient des heures travaillées, base d'évaluation du forfait du marché public. Le musée souhaite contrôler la réalité des heures travaillées, surveiller les conditions de la sous-traitance[113].

Ce marché public contient des dispositions spécifiques, qui s'expliquent par la qualité des œuvres du musée du Louvre : les agents des entreprises sous-traitantes sont l'objet d'une procédure d'agrément ; le bulletin numéro deux du casier judiciaire est examiné. Le recours à la biométrie permet de s'assurer que seuls les agents agréés accèdent au musée du Louvre. L'application biométrique choisie est la reconnaissance palmaire.

L'outil est constitué de bornes associées à un ordinateur qui stocke les informations par une interface. Quand l'image de la main d'une personne est enregistrée dans le dispositif, trois mesures sont réalisées afin d'obtenir la forme de la main en trois dimensions. Le système est paramétré de façon à autoriser un niveau de rejet général plus ou moins élevé en fonction de la sécurité indispensable.

Le dispositif envisagé pour déclencher des ouvertures de porte comporte[114]un ordinateur qui reproduit les transactions : heures de passage en corrélation avec le code de la personne, gestion des alarmes et refus de passage.

Les informations sur les agents agréés des entreprises sous-traitantes sont conservées tant que l'agent est employé par l'entreprise prestataire de services. Les données sur les heures de passage sont conservées pendant une durée d'un an sur support numérique. Cette durée de conservation s'explique par l'obligation qui incombe aux sociétés de garder, pour être éventuellement mis à la disposition des inspecteurs du travail, les éléments constitutifs du

[111] Confidentialité des épreuves

[112] « L'analyse du dossier a permis de considérer que tel était le cas pour l'imprimerie des sujets d'examen et concours, les salles fortes, les coffres et les salles d'archives contenant notamment les dossiers des personnels. La commission a ainsi limité à ces locaux et aux seuls membres du personnel habilités à y accéder le système de reconnaissance des empreintes digitales et la base de données subséquente et a vérifié les mesures prises afin d'assurer la confidentialité des données » 21 ème rapport d'activité de la CNIL, p 116, La Documentation française ? 2001.

[113] Cela entre dans les prérogatives du maître d'ouvrage

[114] De façon optionnelle

temps de travail des employés pendant une année. La CNIL a émis un avis favorable parce que la durée de conservation ne semble pas excessive par rapport à la finalité sécuritaire. Les agents disposent d'un droit d'accès et de rectification.

3) la CNIL admet la proportionnalité au sein des prisons, dans la mesure où les prisonniers sont considérés comme potentiellement dangereux

La biométrie est utilisée pour renforcer la surveillance, à l'occasion de l'accès et lors du retour du parloir.

Un arrêté [115]du 26 juin 2003 porte sur la création de systèmes de reconnaissance biométrique. Une expérimentation avait eu lieu à la prison de la Santé, avec l'avis favorable de la CNIL. L'arrêté de juin 2003 généralise ces mesures.

Le système mis en place par la Direction de l'administration pénitentiaire implique la reconnaissance de la morphologie de la main du prisonnier, couplée à une carte d'identité magnétique. Dès son arrivée dans la prison, le détenu enregistre au greffe un gabarit de la main, qui est stocké avec le nom, une photographie, un numéro d'écrou dans un serveur central[116].

Les données biométriques ne peuvent être communiquées qu'au personnel de l'administration pénitentiaire ; elles sont détruites au moment de la levée d'écrou[117]. Chaque installation est déclarée à la CNIL.

Le recours à la biométrie dans ce contexte tend à lutter contre les évasions par substitution[118].

La généralisation est permise par l'arrêté de juin 2003 mais il y a peu de chance qu'elle devienne une réalité. En effet, ces installations sont coûteuses et il est peu probable que le ministère de la justice équipe chaque prison.[119]La CNIL a rendu un avis favorable parce que la finalité était sécuritaire, parce que la durée de la conservation était limitée dans le temps et parce que les informations ne sont pas stockées sur les cartes d'identité des détenus[120]. Pou la CNIL, il est essentiel que la base centrale qui sera créée soit propre à chaque établissement et ne soit pas interconnectée avec d'autres traitements.

Le personnel pénitentiaire adopte une position nuancée. L'utilisation des techniques biométriques est considérée comme protectrice dans les grands établissements. Dans les petits établissements, le personnel pénitentiaire connaît bien les détenus. Le recours à des techniques biométriques n'a pas de justification. Les associations de soutien aux détenus sont réservées. Les mesures arrêtées et annoncées ont un impact sur l'opinion publique mais n'empêchera pas les évasions qui prendront d'autre formes que les évasions de substitution.[121]

---

[115] du ministère de la justice

[116] Des bornes sont reliées au serveur central

[117] Libération ou transfert vers un autre établissement

[118] « Ce (l'évasion par substitution) n'est pas très courant mais cela s'est produit à quelques occasions. Il fallait donc mettre en place des conditions de sécurité renforcée à ce sujet » déclare Martine Leguedey, de la Direction de l'administration pénitentiaire

[119] « Le ministère de la Justice estime à 50000 euros le budget que devait allouer un établissement à l'installation d'un système de reconnaissance biométrique. Equiper les 187 prisons que compte le territoire français reviendrait donc à près de 9 ?5 millions d'euros ». Transfert.net. 07.2003.

[120] Avis favorable de la CNIL en date du 22 mai 2003 « Pour nous, il y avait deux points sensibles : la durée de conservation des données biométriques et le fait que les informations ne soient pas stockées sur les cartes d'identité des détenus mais sur un serveur central de l'établissement. Comme le texte de l'arrêté présentait toutes les garanties sur ce point, il n'y avait pas lieu d'émettre des réserves »

[121] « Cela sert à rassurer l'opinion publique. Mais les peines prononcées sont toujours plus longues et les conditions de détention de plus en plus difficiles. Ce genre de mesure ne résoudra pas les problèmes de la prison, il ne fait que les déplacer. Si l'on ne s'évade pas par substitution, on le fera d'une autre façon. Et renforcer les mesures de protection nourrit la tendance actuelle qui est aux évasions de plus en plus violentes » déclare Milko, qui édite le site www.prison.eu.org

Il est donc évident que la biométrie sera utilisée dans les prisons, mais il est impossible de déterminer dans quelles proportions .

Ces diverses applications ont une finalité sécuritaire.

B/ Lorque la finalité n'est pas sécuritaire, les autorité de régulation peuvent être réticentes.

1) La finalité peut correspondre à un contrôle de l'accessibilité. Les cantines scolaires constituent un vaste champ de débat en Europe.

   Le collège Jean Rostand de Nice[122] avait choisi une base de données biométriques reposant sur la reconnaissance automatique des empreintes digitales des personnes physiques concernées. Il s'agissait d'associer aux informations administratives et de gestion une représentation codée des empreintes digitales des élèves et des membres du personnel. Cette initiative avait obtenu l'adhésion des parents d'élèves et des représentants du personnel. Néanmoins, la CNIL avait relevé que la constitution d'une base de données d'empreintes digitales était susceptible d'être utilisée à des fins étrangères à la finalité recherchée ; elle avait rendu un avis défavorable, en raison de la disproportion entre le moyen et la finalité recherchée[123].

   Le collège de Carqueiranne, ayant tiré les leçons de l'avis défavorable rendu à l'occasion du projet Jean Rostand, propose un contrôle d'accès basé non pas sur les empreintes digitales, mais sur la technique biométrique du contour de la main. La CNIL rend un avis favorable : le détournement de finalité semble impossible.[124]

   Au Royaume-Uni, le college Venerable Bede de Sunderland[125], créé en septembre 2002, a décidé en juillet 2003 d'installer un système biométrique de reconnaissance de l'iris pour l'accès des élèves à la cantine.

   400 écoles et collèges britanniques recourent déjà à l'infrastructure mise en place par la société écossaise CRB Solutions et au programme d'admission automatisée Impact. Ce système est basé sur l'utilisation d'une carte magnétique que les parents rechargent à un guichet ou par Internet, ce qui dispense les élèves d'avoir de l'argent sur eux et réduit les files d'attente.

   Au Venerable Bede, CRB Solutions ajoute à Impact le procédé de reconnaissance biométrique mis au point par la société américaine spécialiste de l'authentification par l'iris Iridian Technologies.

   Le choix s'est porté sur l'iris plutôt que sur les empreintes digitales pour des raisons d'efficacité[126]. La reconnaissance palmaire n'a pas été envisagée.

   Avant de se mettre à table, les demi-pensionnaires doivent s'identifier grâce à une caméra video. Cette dernière analyse l'image du contour de l'iris et établit une comparaison avec les gabarits scannés stockés dans la base de données du collège.

   L'autorité de régulation en matière de protection des données au Royaume-Uni n'a pas fait connaître son avis. Le collège justifie son investissement, assez lourd,[127]par le souci d'accélérer le service et la volonté d'éviter la perte des cartes de cantine.

---

[122] Délibération 00-015 du 21 mars 2000 portant avis sur le traitement automatisé d'informations nominatives, destiné à gérer l'accès à la cantine scolaire par la reconnaissance des empreintes digitales.

[123] « Si la constitution de bases de données biométriques, y compris d'empreintes digitales peut être justifiée dans certaines circonstances particulières où l'exigence de sécurité et d'identification des personnes est impérieuse, sa mise en œuvre dans un collège, à l'égard notamment de mineurs et aus seules fins de contrôler l'accès à la cantine scolaire est excessive au regard de la finalité poursuivie ». Délibération n° 006015 du 21 mars 2000.

[124] « La technique du « contour de la main » retenue par le collège de Carqueiranne, à la différence de celle des empreintes digitales par le collège de Nice, ne laisse pas de trace dans la vie courante et ne peut donc être détournée de sa finalité première ». Communiqué de presse. CNIL. 15 octobre 2002.

[125] Près de Newcastle

[126] « .. la morphologie des doigts évolue considérablement chez les adolescents alors que le contour de l'iris demeure identique dès le plus jeune âge » déclare David Swanston, directeur de CRB Solutions.

[127] 86000 euros

Par contre, les associations de défense des droits de l'homme militent contre cette mesure, considérée comme attentatoire à la vie privée et aux libertés individuelles. C'est notamment le cas de Privacy International, qui dénonce une mauvaise entreprise de relations publiques.[128]

L'accès aux cantines semble donc générer un besoin réel ou supposé[129], en technique biométrique, mais l'utilisation de ces techniques implique de nombreuses précautions.

2) La finalité peut aussi concerner la vie de l'entreprise et notamment le contrôle des horaires.

Un employeur dispose d'une prérogative de surveillance concernant les horaires auxquels sont assujettis les salariés. Ces derniers se doivent de respecter les horaires collectifs. Le contrat de travail repose sur un lien de subordination.

Les contractants sont de bonne foi. Les obligations réciproques sont basées sur la loyauté. Dans le contexte actuel, la distance entre l'employeur et le salarié s'est considérablement réduite grâce à l'usage des technologies de l'information. La cybersurveillance, dont la CNIL a dénoncé les dérives possibles[130], la biométrie sont autant de moyens possibles mises à la disposition de l'employeur pour contrôler les activités du salarié.[131]

Selon la directive de 1995[132], l'employeur, en tant que responsable du traitement, ne peut agir que si cela est « nécessaire à la réalisation de l'intérêt légitime poursuivi…. à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée » (le salarié).

Les entreprises sont tentées d'utiliser la biométrie pour gérer les horaires. Conscientes de ce besoin, certaines société de biométrie proposent un volet « gestion du temps de travail »[133].

Depuis une vingtaine d'années, l'obligation de pointer sur les lieux de travail, administrations ou entreprises, a pris en compte l'identification. La présentation d'un badge est anonyme. N'importe quel(le) collègue peut présenter le badge, en lieu et place des personnes concernées. C'est pourquoi le recours à des procédés biométriques a été envisagé.

Ainsi, la préfecture de l'Hérault a-t-elle saisi la CNIL d'une demande d'avis relatif à la mise en place d'un traitement automatisé d'informations nominatives destiné à permettre l'authentification des agents travaillant pour la préfecture. Il s'agissait de gérer le temps de travail, d'instaurer un horaire variable grâce à la reconnaissance des

---

[128] « C'est vraiment écraser une fourmi avec un marteau-pilon. Franchement, dans le cas d'un collège, l'utilisation d'une carte magnétique suffit. Ce genre d'initiatives est un exercice de relations publiques… Personnellement, je trouve cela inapproprié, dégradant pour l'enfant et dangereux pour l'avenir » déclare Simpn Davies, president de Privacy International.

[129] Les associations de parents d'élèves, en France comme au Royaume-Uni, sont favorables à l'usage de la biométrie

[130] Rapport sur la cybersurveillance. CNIL. 2001.

[131] « Ce voile tissé de la distance entre le bureau du PDG et le poste de travail du salarié était auparavant opaque. Les nouvelles technologies permettent de le lever chaque jour un peu plus. Il y eut tout d'abord le contremaître puis la carte d'accès, le téléphone et les autocommutateurs, les factures détaillées. Aujourd'hui, s'ajoutent Internet, la messagerie électronique, la biométrie, la cryptographie, la signature électronique, la certification et peut-être le contrôle individuel par puce intradermique ceci, sans parler des potentialités du génie génétique » dans « Cybersurveillance des salariés et règles de preuve devant les Prud'hommes » par Geneviève Folzer et Mathieu Abboud, Strasbourg, 17 janvier 2003

[132] Article 7 f)

[133] Par exemple, GFI Progiciels propose un module de biométrie complémentaire à son offre de logiciels de gestion du temps de travail

empreintes digitales. Ce dispositif a pour objet de pallier les dysfonctionnements du système de badge[134].

Ce dernier est présenté à l'entrée de la préfecture, puis l'agent propriétaire du badge est invité à présenter l'un de ses doigts devant un lecteur d'empreintes digitales. Le procédé d'authentification est fiable[135] : il permet d'éviter les fraudes. La CNIL a dû peser les avantages et les inconvénients de la solution proposée. Parmi les avantages, ont été pris en compte l'adhésion relative du personnel et l'accroissement de sécurité dans un bâtiment soumis au plan Vigipirate. Les représentants du personnel avaient été conviés à une présentation chez un fournisseur. Selon la préfecture, l'impression avait été favorable. L'innovation paraissait équitable. Quant à l'accroissement de sécurité, il est plus contestable puisque la présentation du badge semble répondre aux critères de sécurité dans tous les immeubles soumis au plan Vigipirate. Quant à l'inconvénient, il réside dans le défaut de proportionnalité entre la finalité du contrôle des horaires et la création d'une base de données d'empreintes digitales, qui peut aboutir à un détournement de finalité aux dépens des agents de la collectivité territoriale.[136]Cet avis a été suivi par la préfecture de l'Hérault.

Pour le même motif[137], non plus dans le secteur public, mais dans le secteur privé, une Compagnie aérienne a saisi la CNIL d'une demande de traitement automatisé avec contrôle des empreintes digitales[138].Le procédé était basé sur deux pointeuses biométriques qui identifiaient les employés par leurs empreintes digitales : il s'agissait d'enregistrer le temps de travail réalisé. La CNIL a considéré qu'il y avait un manque de proportionnalité entre la finalité poursuivie et les dangers générés par la constitution d'une base de données d'empreintes digitales, des possibilités de détournement de finalité.

Les personnels pénitentiaires, quant à eux, ont fait connaître leur refus d'étendre l'usage de la biométrie, cantonné jusqu'à maintenant aux déplacements des détenus, à la gestion des horaires de travail[139].

Au sein de l'entreprise, le débat n'est pas clos. La majorité des employeurs sont favorables à l'utilisation de techniques biométriques afin de contrôler les horaires du personnel. Les procédés les plus usités sont le lecteur d'empreintes digitales, l'iris et la reconnaissance palmaires.

A l'opposé, les organismes de régulation en matière de protection des données personnelles et les syndicats représentatifs sont opposés à la maîtrise des horaires par une technique biométrique[140].

La situation n'est pas figée. Il suffit que l'un des acteurs fasse évoluer son point de vue pour que la biométrie contrôle les horaires de travail. C'est vraisemblablement l'un des grands enjeux des années à venir.

---

[134] « Le badge d'accès… ne doit pas pouvoir être utilisé frauduleusement par un agent territorial souhaitant dissimuler l'absence ou le retard d'un de ses collègues. C'est la raison pour laquelle la préfecture souhaite, grâce à un dispositif de reconnaissance des empreintes digitales associé à l'utilisation des badges d'accès, éviter toute utilisation d'un badge par une personne autre que son titulaire ». Délibération n°00-057 du 16 novembre 2000 portant sur un projet d'arrêté présenté par le préfet de l'Hérault concernant un traitement automatisé d'informations nominatives ayant la finalité la gestion du temps de travail des agents de la préfecture.

[135] Pas à 100%

[136] « Un tel objectif ne paraît pas de nature à justifier la constitution d'une base de données d'empreintes digitales des personnels d'une préfecture. Aussi, le traitement pris dans son ensemble n'apparaît-il ni adapté ni proportionné à l'objectif poursuivi ». Délibération n°00-057 du 16 novembre 2000.

[137] Gestion des horaires du personnel

[138] A Roissy-Charles de Gaulle

[139] Ainsi, l'Union générale des surveillants pénitentiaires s'est-elle vivement opposée, à la prison de Fleury-Mérogis, au pointage biométrique.

[140] Big Brother ne semble pas éloigné.

III) La subsidiarité s'applique. Si certains principes sont adoptés dans tous les pays de l'Union européenne, des points de vue différents s'appliquent dans les pays de l'Union européenne.

Cela concerne tant les normes nationales que la problématique des cartes d'identité.

A/ Tous les pays de l'Union européenne ne possèdent pas de lois sur la biométrie

1) Le Québec est, à ce point de vue, à l'avant-garde. En Europe, la majorité des Etats n'a pas de normes spécifiques.
2) Une loi allemande, adoptée à l'automne 2001, comprend un volet sur la biométrie.
   A l'automne 2001, le ministre de l'Intérieur[141] a fait adopter deux séries de mesures destinées à lutter contre d'hypothétiques menaces terroristes. Le premier volet crée de nouvelles taxes pour financer la lutte contre le terrorisme. Le deuxième volet entérine une série de mesures destinées à faciliter les investigations de la police fédérale et des services secrets. Les banques sont tenues de communiquer aux services de renseignements les informations sur les comptes[142] des personnes suspectes. La règle du « témoin à charge »[143] est réintroduite ; il s'agit de faire bénéficier les « repentis » qui acceptent de témoigner contre leurs complices de larges remises de peine[144]. Cette procédure avait été introduite dans le droit pénal allemand dans les années mille neuf cent soixante dix et avait expiré en 1999. Cela signifie que la culture juridique allemande a eu le temps de s'habituer à la pratique des « repentis ».
   Les applications biométriques sont largement utilisées dans les autres mesures. En premier lieu, le fichier des étrangers résidant en Allemagne est développé. Il doit servir de base de données aux services secrets et à la police. Les consulats allemands à l'étranger sont chargés de relever les empreintes digitales des demandeurs de visas. Quand les demandes émanent de pays sensibles, un surcroît de précautions est exigé. Les personnes qui sollicitent l'asile politique sont tenues de fournir un échantillon de leur voix. Un fichier d'enregistrements de la voix des demandeurs d'asile est constitué. La suspicion à l'égard des étrangers[145] et le recours à des moyens d'identification physiologiques sont donc entérinés, malgré les réserves des commissaires à la protection des données. En deuxième lieu, la loi introduit des procédés d'identification biométriques dans les documents d'identité des citoyens allemands afin d'empêcher toute falsification. Dans un premier temps, il avait été question de généraliser l'usage des empreintes digitales. Un vif débat parlementaire a fait évoluer le projet initial. Le choix est ouvert entre l'empreinte digitale, la reconnaissance palmaire, la reconnaissance faciale, l'iris. Deux arguments se sont élevés contre le « tout biométrique » en matière de pièces d'identité : l'usage systématique de la biométrie est susceptible de porter atteinte à la vie privée ; le coût de l'opération[146] n'est pas proportionné à la finalité, la lutte contre le terrorisme.

---

[141] Otto Schily, à l'époque

[142] et mouvements de capitaux en général

[143] Utilisée contre la Fraction Armée Rouge.

[144] « Un meurtrier pourrait voir sa peine réduite à cinq ans de prison au lieu de la perpétuité », « Berlin ficelle son paquet de sécurité numéro 2 » par Lorraine Millot. Libération 1 novembre 2001

[145] Les demandeurs d'asile placés sous la protection de la Convention de Genève peuvent être extradés, si « pour des raisons graves » ils constituent « un danger pour la sécurité de la République fédérale »

[146] « La mise en place de caractéristiques biométriques coûterait des milliards de marks pour un résultat finalement peu efficace au niveau de la lutte contre le terrorisme » « L'Allemagne sur la voie d'une carte d'identité biométrique » par Estelle Dumout, Zdnet France

Malgré ces oppositions, la loi a été adoptée. Elle infléchit au niveau de l'Allemagne le bilan sécurité/ liberté au profit de la sécurité, via, notamment, la biométrie. Cette constatation est d'autant plus significative que l'Allemagne a toujours été particulièrement soucieuse de cet équilibre. Ainsi, l'Allemagne, ou, plus exactement, la RFA, a été l'un des premiers Etats, en 1968, à l'origine d'un texte sur les écoutes téléphoniques[147]. Ce dernier a été révisé en 1998 dans une optique moins favorable aux intérêts des individus. L'Allemagne représente pour l'Union européenne un miroir de l'attelage « attachement aux libertés- importance de la sécurité ».

3) En France, il n'existe pas de normes spécifiques dans le domaine de la biométrie.

3.1) La loi qui porte révision de la loi du 6 janvier 1978 introduit le concept de données biométriques.

3.2) Le rapport Cabal[148] sur « les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre » établit un état des lieux sur les techniques biométriques en France et appelle de ses vœux l'adoption d'une loi sur les techniques biométriques.

3.3) Afin de renforcer la lutte contre l'immigration illégale[149], le recours aux empreintes digitale, déjà permis par une loi de 1997[150], est élargi. Les empreintes digitales et une photo peuvent être relevées mémorisées et faire l'objet d'un traitement informatique à l'égard de tout étranger qui sollicite l'obtention d'un visa. Ces éléments sont obligatoirement relevés quand un visa est délivré.

B/ Il n'existe pas d'unicité en matière de carte d'identité nationale.

1) La carte nationale d'identité existe dans tous les pays de l'Union européenne sauf, au Danemark et au Royaume-Uni
2) A l'exception de l'Italie et de la France, la détention de la carte d'identité est obligatoire. En France, la détention était obligatoire. Depuis 1955, la détention d'une carte d'identité est facultative, mais la grande majorité des Français détient une carte d'identité. Le décret français du 19 mars 1987 a institué une carte d'identité sécurisée ; sa délivrance est généralisée depuis décembre 1995. Etablie sur un papier spécial plastifié, elle comprend plusieurs dispositifs de sécurité destinés à empêcher la falsification. Un projet de carte biométrique [151]est envisagé. La CNIL émet des réserves, soulignant qu'un fichier centralisé avec les empreintes digitales est dangereux pour les libertés individuelles. Elle propose que les informations soient stockées sur la carte proprement dite.
3) La détention d'une carte d'identité permet de circuler librement dans les Etats de l'Union européenne.[152]
4) Les techniques biométriques en matière de cartes nationales d'identité sont utilisées en Espagne, en Italie, au Portugal, en France. La prise des empreintes digitales en Italie est obligatoire depuis peu. ; elle est appliquée depuis octobre

[147] Cf : Arrêt Klass c. RFA, CEDH, 6 septembre 1978 ; la loi de 1968 (G10) est conforme à l'article huit de la Convention européenne de sauvegarde des droits de l'homme

[148] Enregistré à la présidence de l'Assemblée nationale le 16 juin 2003

[149] Loi n°2003-1119 du 26 novembre 2003 afférente à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité

[150] lors de la demande de délivrance d'un titre de séjour

[151] Avec empreintes digitales

[152] L'accord européen sur le régime de la circulation des personnes entre les pays membres du Conseil de l'Europe signé le 13 décembre 1957 autorise les ressortissants des pays ayant ratifié cet accord d'entrer sur le territoire des autres Etats signataires. La Suisse et la Turquie, qui ne sont pas membres de l'Union européenne, ont également signé cet accord.

2002. Néanmoins, la carte d'identité support papier est souvent remplacée depuis l'an 2000 par une carte d'identité électronique. Le décret qui détermine le contenu stipule qu'elle peut contenir les éléments nécessaires au calcul d'une clé biométrique. En France, lors de la constitution de dossier d'une demande, a lieu un relevé des empreintes digitales de la personne concernée. Les enfants de moins de treize ans sont exemptés de cette procédure. L'empreinte digitale ne peut être utilisée que pour permettre une opposition à une tentative d'obtention ou d'utilisation frauduleuse d'une pièce d'identité et l'identification d'une personne physique dans le cadre d'une procédure judiciaire.

5) L'Union européenne se dirige vers une généralisation des cartes d'identité nationales.

5.1) Au Danemark, il convient de noter, à défaut de carte d'identité nationale, le rôle tenu par le fichier national de la population, qui contient tous les éléments d'identification et est utilisé par les administrations.

5.2) Au Royaume-Uni, où, contrairement au Danemark, il n'existe pas de fichier national de la population, la création d'une nouvelle carte d'identité est vivement discutée. La carte d'identité nationale a déjà prévalu lors des deux guerres mondiales du vingtième siècle, pour combattre les ennemis de l'intérieur et de l'extérieur[153]. Elle fut supprimée en 1952. Le 3 juillet 2002, le ministre de l'intérieur de l'époque[154], a proposé l'introduction d'une carte d'identité, qui aurait pour mission la suppression de la fraude[155] aux documents d'identité, la lutte contre l'immigration clandestine et le travail clandestin. Cette carte permettrait aussi un meilleur accès aux services publics de santé et d'éducation. Les techniques biométriques étudiées sont les empreintes digitales et l'iris. Le gouvernement souhaite obtenir l'agrément de la société civile. En effet, une initiative précédente[156] n'avait pas remporté l'adhésion. Après les attentats dirigés en 2001 contre les USA, les sondages d'opinion s'étaient montrés favorables[157]à l'instauration d'une carte d'identité nationale. Ces sondages n'ont aucune valeur scientifique. De plus, l'introduction d'une nouvelle carte d'identité aurait pour conséquence l'amendement de l'Human Rights Act. Une consultation publique a eu lieu au cours du second semestre 2002 et s'est poursuivie jusqu'au 31 janvier 2003.

La carte d'identité coûtera très cher : de 1 à 3 milliards de livres (1,56 à 4,7 milliards d'euros selon le modèle retenu). Le financement serait partiellement alimenté par une augmentation des prix des passeports et des permis de conduire.

Le document qui a donné lieu à consultation offre trois possibilités

- Une carte d'identité réservée à certains groupes sociaux[158], à certaines régions, ou donnant accès à certains services
- Une carte d'identité facultative, mais susceptible d'être proposée à l'ensemble des citoyens
- Une carte d'identité obligatoire

Les deux derniers cas impliquent la mise en place d'un fichier national. Elle serait délivrée à partir de seize ans.

Il est prévu que l'accès à certains services sociaux et de santé soit subordonné à la présentation de la carte.[159]

---

[153] Les déserteurs, les espions et les contrevenants au système de rationnement

[154] David Blunkett

[155] « La fraude coûte au pays chaque année 1,3 milliards de livres (soit 2,03 milliards d'euros) » a déclaré David Blunkett.

[156] En 1996

[157] 85% d'opinions favorables

[158] Les nouveaux immigrants (toujours le contrôle des flux migratoires)

La nouvelle carte serait couplée avec le permis de conduire ou avec le passeport. Elle serait valable pour une durée de dix ans, comporterait un numéro d'identification, les nom, prénom, date et lieu de naissance, l'adresse, la mention de la nationalité britannique, le sexe, le numéro de sécurité sociale, la photographie, la reproduction numérisée de la signature, la profession, l'indication du service qui a délivré le document.[160]

Les organisations de défense des libertés individuelles sont plutôt hostiles à l'instauration d'une nouvelle carte d'identité. Le UK Passport Service a lancé, le 3 décembre 2003, un test auprès de 10000 volontaires, pour la mise en place de cartes d'identité et de passeports contenant des données biométriques. Les procédés utilisés sont soit la reconnaissance faciale, soit l'iris, soit l'empreinte digitale.

Le 26 novembre 2003, le Home Office propose un projet de loi instaurant une carte d'identité qui entrerait en vigueur d'ici 2010 et qui, dans un premier temps, ne serait pas obligatoire. Une base de données nationale stockerait l'élément biométrique, soit une empreinte digitale soit un iris. Néanmoins, il est possible qu'à terme la base de données génétiques soit utilisée par la carte d'identité.

6) En Suisse, qui n'est pas membre de l'Union européenne, mais qui est un pays européen, appelé, à moyen terme, à adhérer à l'Union européenne, l'autorité de régulation en matière de protection des données personnelles, manifeste ses réserves à l'égard de l'utilisation des techniques biométriques dans les documents d'identité. Le Préposé fédéral à la protection des données[161]est hostile à un processus de surveillance généralisée, telle qu'elle est apparue dans d'autres pays occidentaux, sous couvert de lutte contre le terrorisme.[162]Le Préposé demande que, en matière de documents d'identité, les techniques biométriques soient utilisées avec prudence. Il convient d'exclure au moins les données sensibles, notamment la santé.[163]

   En Europe, si les techniques biométriques sont loin d'être généralisées lors de la demande ou de la délivrance des cartes d'identité, cette possibilité existe. Un devoir de veille vigilante s'impose.

Conclusion : Union européenne et divers types de techniques biométriques.

Les instances européennes[164] en matière de protection de protection des données personnelles sont plus ou moins réservées à l'égard des applications biométriques, considérant que certaines d'entre elles sont potentiellement un danger pour la vie privée.

1) Ce sont les empreintes digitales qui sont à l'origine des principales critiques des autorités de régulation.

   La CNIL considère que les empreintes digitales génèrent un risque de traçabilité qui peut être exploité aux dépens des personnes physiques ; en

---

[159] Si cette hypothèse est retenue, la carte deviendra obligatoire

[160] Si on établit une comparaison avec la carte d'identité française, on s'aperçoit qu'il y a beaucoup de points communs. Le projet de carte d'identité britannique comporte en plus le numéro de sécurité sociale et la profession.

[161] Le PFPD

[162] « Des restrictions sont nécessaires, car on en est à un point où la lutte anti-terrorisme ne viole pas seulement les règles de protection des données, mais constitue peu à peu un danger pour les fondements de l'Etat de droit. Le préposé redoute que « des pressions, directes ou indirectes, n'aboutissent à l'introduction en Suisse de mesures de surveillance généralisées, comme c'est le cas dans certains pays » dans « Transfert.net », juillet 2003

[163] Il faut exclure « les données biométriques qui permettent de tirer des renseignements sur la santé ou sur la sphère privée de l'individu » cité dans « Transfert.net », juillet 2003

[164] Groupe dit 29 institué par la directive de 1995

conséquence,[165] une base de données d'empreintes digitales peut être utilisée à d'autres fins que l'objectif poursuivi à la création. Le détournement de finalité est possible.

C'est pourquoi les empreintes digitales sont surtout utilisées à des fins d'identification policière : passeports, visas ou dans le cadre d'un besoin spécifique dans le domaine de sécurité. Enfin, les empreintes digitales peuvent servir à une opération électorale. En France, à l'occasion des élections du printemps 2002,[166]la mairie de Mérignac souhaitait expérimenter dans un bureau , un dispositif de vote électronique qui impliquait l'utilisation de cartes à microprocesseur comportant les empreintes digitales des électeurs. Ces derniers sont volontaires pour tenter l'expérience, sur le mode électronique comme sur le mode traditionnel. Cette application s'inscrit dans le cadre d'un projet européen de vote électronique « E-Poll »[167] financé par la Commission européenne, au titre d'un programme de recherche[168].

Ce projet stipule que les électeurs volontaires disposent de cartes à microprocesseur avec empreintes digitales. Les électeurs s'authentifient en introduisant leur carte à puce dans un lecteur et en apposant leur index sur un capteur relié à un ordinateur. L'identité est vérifiée par la confrontation des empreintes ; quant à l'ordinateur, il est relié au serveur conservant la liste électorale et il vérifie si l'électeur est bien sur la liste. L'électeur se voit ensuite attribuer un certificat de vote qui est enregistré dans la carte dont il est porteur. Pour voter électroniquement, il insère sa carte dans un deuxième ordinateur avec écran où apparaissent les noms des candidats, appuie sur le nom choisi (expression du vote), appuie son index sur un scanner connecté au serveur qui gère la liste d'émargement (validation du vote).

L'enregistrement des empreintes digitales permet de s'assurer de l'identité des électeurs et de l'unicité du vote. La CNIL accepte le recours aux empreintes digitales dans la mesure où aucun fichier n'est constitué. Encore émet-elle un avis mitigé bien que favorable[169].Cet avis est assorti de réserves : il doit être fait mention de l'utilisation des cartes à microprocesseur ; il sera clairement indiqué que les empreintes digitales ne feront l'objet d'aucun fichier nominatif ; seuls, les personnels habilités de la mairie, de la Préfecture, des prestataires de services sont à même d'accéder, si le besoin se manifeste[170] aux informations nominatives indispensables à la constitution de la liste électorale. Il apparaît donc que le recours aux empreintes digitales, bien qu'assez répandu pour répondre aux besoins des ministères de l'intérieur européens est le procédé biométrique qui génère le plus de risques au regard de la directive de 1995 sur la protection des données personnelles.

2) La reconnaissance palmaire : est le procédé le mieux accepté par les autorités de régulation européennes en matière de protection des données personnelles. La reconnaissance de la main s'appuie sur une image en trois

[165] « les empreintes digitales…. Des traces qui peuvent être explotées à des fins d'identification des personnes à partir des objets les plus divers que l'on a pu toucher ou avoir en main » CNIL, 21ème rapport d'activité, p 113, La Documentation française, 2001

[166] Elections présidentielles et législatives.

[167] Electronic Polling System for Remote Voting Operations

[168] Information Society Technology

[169] cf : sémantique : le recours aux empreintes digitales *peut être admis.* Délibération n° 02-015 du 14 mars 2002 portant avis sur un projet d'arrêté présenté par la mairie de Mérignac

[170] « en tant que de besoin ». Délibération n° 02-015 du 14 mars 2002

dimensions.[171]Elle n'appartient pas aux données biométriques qui laissent des traces et qui peuvent donner lieu à identification. C'est pourquoi, en France, la CNIL considère que la reconnaissance palmaire présente des garanties[172] pour les libertés individuelle, pour la protection de la vie privée. Les autres autorités de régulation européennes sont favorables à la reconnaissance palmaire, pour des raisons identiques à la CNIL. Au Québec, les usagers de l'université de Montréal sont reconnus grâce à la forme de leurs mains.

3) La reconnaissance faciale : donne lieu à des développements, surtout depuis les attentats du 11 septembre 2001, si médiatisés. Elle se base sur les caractéristiques principales du visage pour construire une carte du faciès. Il convient d'établir une distinction entre la reconnaissance de visage fixe et la reconnaissance de visage mobile. L'identification d'un sujet fixe est assez fiable. L'identification d'un sujet mobile induit un taux d'erreurs élevé. L'usage de cette application est assez répandue. Elle n'exige pas le consentement des personnes concernées, ce qui satisfait les institutions policières et induit des critiques de la part des autorités de régulation. En France, la CNIL n'a instruit aucun dossier de reconnaissance faciale. En Belgique, la police fédérale a validé, en mai 2002, l'installation d'un système de reconnaissance faciale au sein de ses bureaux[173]. Des systèmes voisins ont été instaurés dans d'autres Etats européens[174]. Déjà, en 2001, Milipol[175] propose de nombreuses caméras de démonstration. Les aéroports utilisent fréquemment ce procédé, qui est dénoncé par les organismes de défense des droits de l'homme. Ainsi, l'aéroport international de Zurich a testé un système de reconnaissance faciale. La même démarche a été suivie dans des aéroports néerlandais et britannique.
4) L'iris : c'est une technique biométrique efficace. L'iris est unique ; les deux iris de la même paire d'yeux sont différents. Les iris de jumeaux monozygotes ne sont pas identiques. Un iris, sur le plan de la biométrie, est extrêmement complexe[176]. Le taux d'erreur est proche du zéro. Cependant, il convient, pour parvenir à ce résultat, de se procurer des systèmes haut de gamme[177]. D'après une étude du Gartner, les critères retenus pour juger de la qualité d'une technique biométrique sont les suivants : non-intrusivité, le niveau de sécurité, le coût, facilité d'utilisation. C'est la reconnaissance par l'iris qui présente la notation la plus avantageuse. Le seul inconvénient réside dans la cherté de l'application.

   Toutefois, pour les tenants de l'irodologie[178], « l'iris est le raconteur des histoires de notre monde intérieur. Il révèle comment nos pensées et notre

[171] « Quelques traits caractéristiques sont gardés en mémoire, la taille et la largeur des doigts, l'espace entre les différentes parties de la main » JDNet solutions, « Biométrie : six moyens d'identifier un utilisateur, 26 août 2002

[172] Néanmoins, la CNIL a traité moins d'une dizaine de demandes d'avis concernant la reconnaissance palmaire.

[173] Dans ce système, le logiciel Face IT de Visionics permet de comparer le visage d'un suspect à ceux stockés dans une banque de données nationale (BNG) de 250000 images. Pour qu'une personne figure dans la banque de données, il faut qu'elle ait commis une infraction, qu'elle ait été arrêtée et que son identité ait été contrôlée. La personne dont l'image est stockée n'a pas obligatoirement été jugée.

[174] Par exemple, dans l'aéroport de Keflavik en Islande

[175] Salon de la sécurité intérieure des Etats

[176] Il est possible de distinguer jusqu'à deux cent quarante quatre points de comparaison

[177] Les systèmes de reconnaissance de l'iris les moins évolués sont susceptibles d'être trompés par une image ou une lentille qui reproduit le dessin de l'iris. Les systèmes les plus évolués peuvent déjouer ces reproductions, notamment en contrôlant que l'iris change de taille avec l'intensité de la lumière.

[178] Qui n'est pas évaluée comme une science

mode de vie influencent notre corps physique »[179]. L'irodologie prétend faire le diagnostic de l'état de santé d'une personne par l'étude de l'iris. En admettant que l'irodologie ait un quelconque fondement, la détection de l'iris, y compris par des non-médecins[180] présente un danger pour la protection des données personnelles. En effet, la santé fait partie des données sensibles, qui, sauf exceptions, ne doivent pas donner lieu à la constitution de fichiers nominatifs, de bases de données.

5) La rétine : une lumière infrarouge de forte intensité scanne l'iris. La technique est efficace mais elle porte atteinte aux libertés individuelles. En principe, seuls, les ophtalmologues, à des fins médicales peuvent réaliser ce type d'examens.

   Un rapport a été établi par Marc Chassé[181]. D'après lui « le balayage de la rétine, ou de l'iris, permet de savoir si une personne est droguée ». Les renseignements médicaux, qui peuvent être ainsi collectés, rentrent dans la catégorie des données personnelles sensibles. C'est pourquoi la reconnaissance par la rétine est très peu utilisée par les décideurs, sauf dans certains milieux carcéraux.

6) L'ADN : c'est la technique biométrique la plus fiable, mais elle est intrusive, encore plus que la reconnaissance par la rétine. Elle n'est donc utilisée que par les milieux policiers et donne lieu à bien des critiques. Par exemple, la base de données de la police anglaise a été initiée avant que la loi devant avaliser ce stockage n'ait été votée. Les policiers sont invités à prélever un échantillon[182]d'ADN sur toute personne arrêtée, quel que soit le crime ou le délit dont elle est suspectée et qui n'a pas encore été jugée. La commission chargée par le gouvernement de fixer les lignes directrices de la police génétique de la Grande-Bretagne a émis des réserves. Pour la présidente de cette commission, le contrôle de la base de donnée devrait être confiée à une entité indépendante et non à la police. De plus seuls les individus jugés et reconnus coupables devraient être fichés. Le prélèvement d'ADN porte atteinte à la présomption d'innocence. Quant à la base de données, elle peut être considérée comme contraire à la convention européenne des droits de l'homme.

   Les diverses applications biométriques ne sont pas sans poser de nombreuses questions. Les industriels, d'une part, les autorités de régulation dans le domaine de la protection des données personnelles, d'autre part vont faire évoluer les termes de la problématique.

[179] Bernard Jensen, zélateur de l'irodologie
[180] Qui ne sont pas tenus au secret professionnel
[181] Analyste informatique québécois.
[182] La base de données ADN de la police anglaise a reçu en 2003 le Big Brother Awards du « projet le plus effrayant de l'année »

DEUXIEME MODELE : LE Canada

Nous étudions dans ce chapitre l'Etat fédéral canadien et les provinces canadiennes. Nous excluons volontairement de cette étude le Québec, plus avancé que l'Etat fédéral et qui applique sa propre législation, proche de l'Union européenne[183].

Au Canada (Etat fédéral) , il n'existe aucun texte spécifique relatif à la biométrie. Les techniques biométriques sont régies par les textes généraux sur les « renseignements personnels ».La protection de la vie privée se réfère à la Charte canadienne, qui accorde aux citoyens le droit de se déplacer sans présenter leurs papiers à un représentant de l'autorité.

Deux normes jouent un rôle éminent : la loi sur la protection des renseignements personnels et la loi sur la protection des renseignements personnels et les documents électroniques.

La loi sur la protection des renseignements personnels a été adoptée en 1985. Elle définit la collecte, la conservation des renseignements personnels, l'accès aux renseignements personnels. Elle crée l'organisme de régulation, le commissariat à la protection de la vie privée, dévolu à une seule personne[184]. Le dernier commissaire à la protection de la vie privée était George Radwanski[185] ; Robert Marleau[186]lui a succédé dans une fonction d'intérim.

La loi sur la protection des renseignements personnels et les documents électroniques a été préparée et discutée à partir de 1998, adoptée le 13 avril 2000[187]. Elle concerne exclusivement le secteur privé et a pour but de s'adapter à la société de l'information, à l'Internet. Elle protège surtout les consommateurs, auxquels est donnée l'assurance d'une protection en

---

[183] Cf : supra : Québec
[184] Entourée de collaborateurs
[185] Mai 2003
[186] qui a une grande expérience de la vie parlementaire Cf : communiqué du 18 Septembre 2003
[187] Sanction royale le 13 avril 2002

matière de confidentialité, d'intégrité, d'authenticité des transactions électroniques[188]. Les dispositions de la loi s'inspirent du code type pour la protection des renseignements personnels de l'Association canadienne de normalisation.[189]Elles concilient ou tentent de concilier les intérêts des entreprises qui veulent recueillir, conserver, utiliser des renseignements personnels et les droits des personnes physiques qui peuvent exercer un contrôle sur les renseignements personnels qui les concernent. Dans un premier temps, les dispositions s'appliquent dans le secteur privé assujetti à la réglementation fédérale ainsi qu'à tout renseignement commercial utilisé dans le cadre d'activités commerciales interprovinciales. A partir du 1er janvier 2004,elles s'étendent à tous les renseignements personnels recueillis, divulgués dans le cadre d'activités commerciales. Si une province adopte une loi similaire, elle est exemptée de l'application de la loi fédérale[190].

La loi introduit aussi le concept de signature électronique sécurisée qui peut être utilisée dans le cadre de transactions électroniques au sein de l'administration fédérale Elle précise les modalités selon lesquelles les tribunaux évaluent la fiabilité des documents électroniques présentés comme preuves[191]. L'articulation de la loi est la suivante : Partie 1 : protection des renseignements personnels dans le secteur privé ; Partie 2 : documents électroniques ; Partie 3 : modification de la loi sur la preuve au Canada.

La lecture de cette loi permet de constater que la même norme traite de la protection des données personnelles et de la signature électronique, secteurs qui sont tous deux afférents à la biométrie mais qui sont traités séparément au sein de l'Union européenne[192]. D'autre part, le droit fédéral canadien privilégie le secteur privé et prend en compte le droit de la consommation en tant que tel.

L'état fédéral prend en compte la diversité des cultures provinciales ; un projet de carte d'identité fédérale donne lieu à controverse.

I/ L'état fédéral prend en compte la diversité des cultures provinciales.

Les provinces élaborent des lois en référence avec la LPRPDE[193]. Le commissaire à la protection de la vie privée fait connaître son avis

A) L'Ontario : soumet un avant-projet de loi au commissaire à la protection des données. Le texte, selon le commissaire, ne peut être considéré comme similaire à la LPRPDE[194]. Déjà, en 1997, une loi sur le programme « Ontario au travail » autorisait la collecte et l'utilisation de l'information biométriques dans quelques cas, notamment pour empêcher qu'une personne soit inscrite plusieurs fois comme auteur d'une demande d'aide sociale. Cette loi interdisait la communication de renseignements biométriques à un tiers[195].Dans tous les cas, les renseignements biométriques devaient être recueillis directement, au su de l'intéressé(e). Ils ne pouvaient servir d'identificateur de dossier unique ni être stockés dans une base de données centrale. Le nouveau projet de loi pose plusieurs questions.

1) Le consentement : la protection des renseignements personnels implique le droit de contrôler l'accès à sa personne et aux renseignements personnels la concernant. Le consentement doit être au cœur de la loi. La notion de consentement exprès apparaît dans le projet, notamment sur la collecte de renseignements personnels dans le domaine de la

[188] La majorité des Canadiens souhaitaient que les renseignements personnels fussent protégés dans l'Internet.
[189] CSA ; passage de l'autorégulation à la régulation.
[190] Exemple du Québec
[191] Dans ce domaine aussi, l'Etat fédéral est très en retard sur le Québec
[192] Directive de 1995, 1997, 2002, pour la protection des données personnelles, directive de 1999 pour la signature électronique, et notamment la signature électronique avancée.
[193] Loi sur la protection des renseignements personnels et les documents électroniques
[194] « J'interpréterai une loi comme essentiellement similaire si elle offre un degré et une qualité de protection de la vie privée égaux ou supérieurs à la LPRPDE » George Radwanski, 8 avril 2002

[195] sauf en vertu d'une ordonnance d'un tribunal, d'un mandat.

santé par une organisation qui n'est pas un dépositaire de renseignements sur la santé. Néanmoins, le consentement n'est pas obligatoire pour la collecte, l'utilisation, la divulgation de renseignements personnels. Or, la collecte, l'utilisation, la divulgation ne devraient être permises sans consentement des personnes physiques que dans des cas exceptionnels. Ce n'est pas le cas dans le projet qui autorise la collecte, l'utilisation, la divulgation dans un grand nombre d'occurrences.

2) Les droits d'accès et de correction : le projet établit une distinction entre les renseignements afférents à la santé et les autres renseignements personnels.
   L'accès peut être refusé si les renseignements ont trait à la sécurité, à la défense du Canada, à la conduite d'affaires internationales, si les renseignements sont relatifs à l'exécution d'une loi, d'un règlement, ou à la conduite d'une enquête sur l'exécution d'une loi ou d'un règlement .Il est difficile d'établir si les renseignements entrent dans ces catégories[196]. Par ailleurs, il devrait exister un processus permettant de surveiller l'utilisation de ces dispositions.
   Enfin, le projet permet à une organisation ou à un dépositaire de renseignements sur la santé de réclamer le paiement de « droits raisonnables ». Le droit d'accès ne doit pas être limité par le coût[197]. C'est pourquoi la LPRPDE ne prévoit que des « droits minimes »
3) Le recours : Les contrevenants doivent être tenus de mettre un terme à la pratique répréhensible. Les dispositions prévues dans le projet diffèrent sensiblement[198] de la LPRPDE mais elles sont appropriées.
4) Les renseignements personnels sur la santé : sont un sujet particulièrement sensible. Les patients s'attendent à ce qu'on ne recueille pas de renseignements personnels sur leur santé, sauf pour les soigner. Ils ont le droit d'exiger que ces renseignements personnels ne soient pas utilisés à leur détriment. Le projet de loi ontarien est ambivalent.

4.1) Une protection est instituée : les renseignements génétiques impliquent un consentement exprès et distinct de la collecte, de l'utilisation, de la divulgation

Un consentement exprès est exigé pour la collecte de renseignements personnels sur la santé par une personne morale qui n'est pas dépositaire de santé.

4.2) Le consentement n'est pas nécessaire dans un trop grand nombre de cas :

- Plusieurs utilisations, comme l'affectation des ressources, la surveillance et l'évaluation des programmes, ne sont pas directement liées aux soins dispensés et devraient être anonymisées.
- La personne morale peut divulguer des renseignements personnels sur la santé aux fins de l'administration, de l'exécution ou d'une enquête relative à l'exécution d'un « règlement municipal »
- Le dépositaire peut divulguer des renseignements personnels sur la santé à des fins de recherche
- Les exploitants d'un service d'ambulance peuvent communiquer des renseignements personnels sur la santé pour les fins prévues par la « loi sur les ambulances ».
- Un dépositaire de renseignements personnels sur la santé est tenu de divulguer au ministre de la santé les renseignements personnels sur la santé à des fins de surveillance et de vérification des demandes de paiement des soins de santé financés par le ministère

---

[196] « Un détaillant un organisme de bienfaisance ou un praticien de la santé risque peu d'avoir l'expertise voulue pour établir si la communication de certains renseignements menacera la sécurité nationale » Rapport du commissaire à la protection de la vie privée. Avril 2002

[197] « La disposition permettant de renoncer aux droits si le paiement devait causer des difficultés financières à l'auteur de la demande n'est pas une solution suffisante. Bien au contraire, cette disposition pourrait, de fait, obliger le particulier à divulguer de nouveaux renseignements pour faire la preuve de ses difficultés financières » Rapport du commissaire à la protection de la vie privée.

[198] En raison des pouvoirs du commissaire ontarien de prendre des ordonnances

5) Renseignements personnels sur la santé et la recherche : dans ce domaine, un équilibre doit être trouvé entre l'intérêt général et l'intérêt particulier.
La LPRPDE permet aux personnes morales d'utliser un renseignement personnel à l'insu de l'intéressé si l'utilisation est réalisée à des fins statistiques ou à des fins d'étude[199].
La confidentialité doit être assurée. Les renseignements personnels sur la santé ne doivent jamais être communiqués aux employeurs, aux assureurs, aux proches de la personne physique[200]. Par contre, les renseignements personnels sur la santé peuvent être divulgués à un chercheur[201], à condition que le projet soit examiné et approuvé par une commission d'éthique de la recherche.

B) La Colombie-Britannique : en mai 2003, après que la province de Colombie- Britannique ait soumis un projet de loi au Commissaire à la protection de la vie privée, George Radwanski fait part de ses observations

1) Le consentement : le projet de loi fait allusion au consentement implicite, une forme de consentement que le Commissaire à la vie privée considère comme faible.[202]Le consentement explicite, écrit, est omis. C'est dangereux puisque les personnes morales sont autorisées à penser que tout est basé sur le consentement implicite. La LPRPDE recommande vivement l'utilisation du consentement explicite en ce qui concerne la collecte, l'utilisation, la communication de renseignements sensibles.[203]
2) Les renseignements personnels et l'emploi : la plupart des personnes physiques passent le plus clair de leur temps sur leur lieu de travail. Or, le projet de loi permet la collecte, l'utilisation, la communication de renseignements personnels des salariés sans leur consentement. Les employés sont privés de tout contrôle sur les renseignements personnels. Un employeur peut croire raisonnable de recueillir et de communiquer des renseignements sur l'état de santé, la religion, l'orientation sexuelle des employés. Une fois le fait accompli, le salarié pourrait se plaindre que la collecte et la communication n'étaient pas raisonnable, en vain.[204]La LPRPDE n'établit aucune distinction entre les renseignements recueillis dans le cadre de l'emploi ou dans le cadre d'activités commerciales.
3) Le projet de loi offre moins de garanties en matière de droit d'accès et de correction. En matière de droit d'accès, une limitation existe : les personnes physiques ne peuvent avoir accès aux renseignements qui les concernent si cela a pour effet de révéler l'identité de la personne qui a fourni l'information.[205]Elles ne peuvent non plus vérifier l'exactitude des renseignement personnels

---

[199] La LPRPDE détermine quatre critères pour l'utilisation de ces renseignements personnels sur la santé sans consentement :
- Les fins, dans le cas de la recherche, ne peuvent être réalisées sans que le renseignement soit utilisé
- Le renseignement est utilisé dans des conditions qui assurent la confidentialité
- Le consentement est pratiquement impossible à obtenir
- L'organisation, la personne morale doivent informer le commissaire de l'utilisation avant de la faire

[200]Cela signifie également que seuls le médecin ou « un fournisseur de soins de santé primaires peuvent communiquer avec la personne physique »

[201] Sans le consentement de l'intéressé

[202] « qui n'est acceptable que dans certaines circonstances limitatives » Rapport du Commissaire à la vie privée sur le projet de loi en Colombie-Britannique. Mai 2003

[203] « Un ensemble de loi qui permettrait à des organisations de compter entièrement sur le consentement implicite offrirait un niveau considérablement inférieur de protection que la LPRPDE » Rapport du Commissaire à la vie privée sur le projet de loi en Colombie-Britannique. Mai 2003

[204] « Une fois qu'on a enfreint la vie privée, on ne peut inverser le processus ». Rapport du Commissaire à la vie privée sur le projet de loi de Colombie-Britannique. Mai 2003

[205] « Par exemple, une personne ne serait pas en mesure d'avoir accès à des commentaires négatifs d'un collègue ou d'un superviseur si cela révélait l'identité de la personne qui a fait les commentaires ». Rapport du Commissaire à la vie privée sur le projet de loi en Colombie-Britannique. Mai 2003

Ainsi, la loi n'exige pas, lorsque l'exactitude de l'information est en cause, que la personne morale qui contrôle l'information informe d'autres personnes qui ont accès à l'information de la teneur du conflit.

4) Le projet de loi permet la collecte, l'utilisation, la communication sans le consentement pour les besoins d'une enquête ou de procédures. Le libellé du projet de loi est trop vague. La définition du terme « enquête » est beaucoup plus générale que celles de la LPRPDE. Selon la LPRPDE, la notion d' « enquêtes » est limitée à « sur la violation d'un accord ou la contravention du droit fédéral ou provincial ».
   Dans le projet de loi, l'enquête peut être liée « à des circonstances ou à un comportement qui pourrait entraîner un recours ou un redressement en vertu d'un texte législatif, de la common law ou en équité »
   Ces définitions sont préjudiciables au projet de loi dont elles abaissent le niveau de protection.
   Le projet de loi de la Colombie-Britannique n'est pas considéré comme similaire à la LPRPDE.

C) L'Alberta : un projet de loi est présenté au Commissaire à la protection de la vie privée, qui fait connaître ses observations en mai 2003.

1) Le pouvoir discrétionnaire conféré au lieutenant gouverneur en conseil[206] : le lieutenant gouverneur en conseil peut, d'après le projet de loi, édicter des règlements afférents à de nombreux sujets, notamment :

- l'octroi d'un consentement
- les formalités à suivre pour présenter des demandes d'accès et y répondre
- les circonstances dans lesquelles des renseignements personnels peuvent être recueillis, utilisés ou communiqués sans consentement.
- Les renseignements personnels non visés par la loi.
- Ce pouvoir peut réduire considérablement le niveau de protection offert par le projet de loi. Les pouvoirs de réglementation devraient être limités à des questions administratives imprévues.

2) Les dispositions d'antériorité : le projet de loi stipule que les renseignements recueillis avant l'entrée en vigueur de la loi « seront réputés avoir été accueillis avec le consentement d'une personne en question ».
   Cette approche est incompatible avec celle de la LPRPDE : pour utiliser ou communiquer des renseignements recueillis avant l'entrée en vigueur de la loi, les personnes morales doivent obtenir leur consentement.

3) Les droits des salariés[207] ne sont pas bien protégés. Le projet de loi permet expressément la collecte, l'utilisation, la communication de renseignements personnels relatifs aux employés sans leur consentement. De plus, le projet de loi ne prévoit pas que les employés doivent être informés a posteriori.[208]. Le projet de loi exige que la collecte, l'utilisation, la communication des renseignements personnels concernant les employés soient « raisonnables ». Le Commissaire à la protection de la vie privée remarque que l'adjectif « raisonnable » épouse étroitement le point de vue des employeurs.[209]Il n'existe aucun équilibre entre le point de vue des employeurs et le point de vue des employés.

---

[206] Le cabinet

[207] Le texte canadien préfère employer le terme « employés »

[208] « Par conséquent, les employés peuvent ne pas avoir la moindre idée que des renseignements qui les concernent ont été recueillis, utilisés ou communiqués, pouvant être complètement privés du droit de se plaindre » Rapport du Commissaire à la protection de la vie privée sur le projet de loi d'Alberta. Mai 2003.

[209] « Presque toute atteinte à la vie privée d'un salarié peut être jugée « raisonnable » ». Rapport du Commissaire à la protection de la vie privée sur le projet de loi d'Alberta. Mai 2003.

Pourtant, la LPRPDE s'applique depuis deux ans dans 15000 entreprises et ces dernières ont pu gérer efficacement leur main d'œuvre.

4) Droit d'accès et de correction : les personnes physiques ne peuvent faire valoir leur droit d'accès si cela a pour effet de révéler l'identité de la personne qui a fourni l'information.
   En outre, une personne peut se voir refuser l'accès à des renseignements parce que la communication risquerait de priver la personne morale[210]de ce genre de renseignements pour l'avenir.
5) Les droits à payer : le projet de loi évoque des « droits raisonnables », alors que la LPRPDE exige « des droits minimes ». La différence est importante.
6) Le projet de loi permet la collecte, l'utilisation, la communication de renseignements, sans consentement, à des fins d'enquête ou de procédures judiciaires. Or, le terme « enquête » est beaucoup plus vaste que la notion envisagée dans la LPRPDE. La définition du projet de loi comprend les enquêtes sur des « circonstances ou comportements qui pourraient donner lieu à des recours en droit ».
   En résumé, le projet de loi permet trop souvent la collecte de renseignements sans consentement.
7) Les organismes sans but lucratif ; le projet de loi permet au lieutenant gouverneur en conseil d'exempter les organisations sans but lucratif. Or, certains organismes sans but lucratif recueillent des renseignements très sensibles, notamment sur la santé des personnes physiques. Permettre à des sociétés sans but lucratif de communiquer de tels renseignements sans consentement, à des fins lucratives équivaut à accorder un niveau de protection moindre que celui garanti par la LPRPDE.
   Le projet de loi concernant l'Alberta ne peut être considéré comme similaire à la LPRPDE.

II/Un projet de carte d'identité canadienne donne lieu à controverse.

Le ministère fédéral de la citoyenneté et de l'immigration envisage de rendre obligatoire une carte d'identité avec indications biométriques. Un débat public est instauré. Le Comité permanent de la citoyenneté et de l'immigration a été chargé de mener et d'animer ce débat.

A) La Commission d'accès à l'information du Québec a fait part de ses réticences. Elle admet que des pays démocratiques ont introduit des cartes d'identité obligatoires. Au Canada, et notamment au Québec, les citoyens sont d'avis qu'une carte d'identité obligatoire induit des risques pour la vie privée. Elle peut constituer un premier pas vers une société de surveillance[211]. Il convient de protéger la vie privée des citoyens. La mise en place d'une carte d'identité implique la création de banques de données regroupant des informations sur l'ensemble de la population. La technologie de l'information permet de relier plusieurs banques de données, ce qui pourrait déboucher sur une surveillance quasi totale des Canadiens quant aux activités quotidiennes. Quant à l'utilisation des techniques biométriques, elle est incompatible avec l'état du droit du Québec. Le passeport suffit à identifier les personnes physiques[212].

---

[210] Le texte canadien préfère utiliser l'expression « organisation »

[211] « Trop de personnes ont des inquiétudes à cause de la multiplication des échanges de renseignements et craignent que les cartes d'identité projetées en facilitent l'accroissement. L'omniprésence de l'Etat dans la vie privée des personnes et le spectre d'une société de surveillance en inquiètent plus d'un » Commission parlementaire de l'Assemblée nationale du Québec sur la carte d'identité.1998

[212] « Il existe déjà un document très officiel dans chaque pays, le passeport, et c'est encore la meilleure preuve de la citoyenneté qu'on puisse trouver. J'ai de très sérieuses réserves par rapport au caractère obligatoire du projet soumis par M. Coderre, et je n'ai pas l'assurance qu'il garantira aux citoyens la protection de leurs renseignements personnels » Mme Courchesne. 2003

B) A Ottawa, la carte d'identité nationale s'inscrit dans le cadre d'une politique de sécurité.

1) Les relations privilégiées entre le Canada et les USA ont joué un rôle dans le projet de création d'une carte nationale d'identité[213]. Cette dernière faciliterait les vérifications douanières et permettrait un meilleur contrôle des frontières.

2) Cette carte fédérale d'identité ne sera adoptée qu'à l'issue d'un long processus démocratique. Le Comité permanent de la citoyenneté et de l'immigration rend ses conclusions à l'automne 2003. Un forum national est instauré en Octobre 2003, avec des experts et des représentants de la société civile. La carte d'identité comprendrait des marqueurs biométriques, empreintes digitales ou iris. L'adoption d'une carte d'identité biométrique permettrait de lutter contre les vols d'identité, vols d'adresse, de cartes de crédit et de débit, documents contrefaits. Selon le ministre canadien de la citoyenneté et de l'immigration, une carte canadienne biométrique avec données biométriques pourrait éviter aux Canadiens d'être fichés aux USA.

3) Un problème juridique doit trouver une solution : l'état civil est, jusqu'à présent, l'apanage des provinces. L'institution d'une carte fédérale d'identité induirait une réforme constitutionnelle.

4) Les critiques :

4.1) Le coût de la mesure : serait très élevé, trop élevé[214]

4.2) Une finalité qui ne serait pas atteinte : les fraudeurs trouveront le moyen de contourner les mesures de contrôle[215].

4.3) Une menace contre les libertés : l'ancien Commissaire à la protection de la vie privée, George Radwanski, avait qualifié le projet « d'ingérence d'une ampleur inimaginable ». L'actuel Commissaire à la protection de la vie privée, Robert Merleau, est préoccupé par l'instauration d'un système de sécurité biométrique. Certaines techniques biométriques sont plus intrusives que d'autres. Gerald Keddy, membre du Comité permanent de la citoyenneté et de l'immigration redoute que la biométrie faciale soit adjointe à l'iris et aux empreintes digitales comme application biométrique[216]. Les dérives sont toujours possibles en matière de libertés publiques. Julius Grey, spécialiste de la charte canadienne des droits considère que la carte d'identité fédérale n'est pas dangereuse en soi, mais que la centralisation des données personnelles peut induire des dysfonctionnements[217].

Les critiques canadiennes peuvent nourrir la réflexion européenne, si l'on songe que la grande majorité des Etats européens ont une carte d'identité et certains une carte biométrique.

---

[213] « D'ici là, les Etats-Unis vont mettre en application un système sévère qui contrôlera les entrées et les sorties du pays et ils vont constituer leur propre banque de données d'empreintes digitales. Au lieu de subir ce qui pourrait venir de l'extérieur, ne vaudrait-il pas mieux trouver une solution typiquement canadienne ? » Denis Coderre, ministre de la citoyenneté et de l'immigration. 2003

[214] Un comité de la Chambre des communes a évalué à 7 milliards de dollars la mise en place d'une carte d'idendité nationale biométrique.

[215] « Il faut être naïf pour penser que le vol d'identité va diminuer à cause d'une carte d'identité nationale » déclare Denis Barrette, membre de la Ligue des droits et libertés du Québec. 2003

[216] « La biométrie faciale est une grande invasion dans votre vie personnelle. Nous parlons vraiment ici de Big Brother. Une caméra dans la rue, dans un aéroport, dans une banque, um magasin, va pouvoir prendre votre biométrie faciale et vous identifier » Gerald Keddy, membre du Comité permanent de la citoyenneté et de l'immigration.

[217] « Et même si ce n'est pas l'intention de M.Coderre, c'est certain qu'il va y avoir des abus d'ici cinq ou dix ans » « Dans cinq, dix ou quinze ans, quand il va y avoir un autre gouvernement ou qu'il va se produire une situation d'urgence qui dépasse celle du 11 septembre, les gens vont pouvoir utiliser ces données pour de mauvaises raisons. Il y a toujours un danger » déclare Julius Grey, 2003

III) Le programme CANPASS-Air : c'est une initiative conjointe de Citoyenneté et Immigration Canada[218]et de l'Agence des douanes et du revenu du Canada[219]. Ce programme tend à faciliter l' entrée rapide au Canada, par voie aérienne, des voyageurs qui présentent un faible risque en termes de sécurité. Le procédé biométrique utilisé est le contrôle de l'iris.

TROISIEME MODELE : LES USA

Aucun texte ne consacre expressément aux USA- Etat fédéral- le droit à la vie privée. La Cour suprême a néanmoins dégagé l'existence d'un tel droit des premier, troisième, quatrième, cinquième et quatorzième amendement. Le premier amendement protège la liberté d'expression et d'association. Le troisième amendement interdit aux militaires de « se dissimuler dans les maisons ». Le quatrième amendement protège les citoyens contre les enquêtes et les saisies arbitraires. Le cinquième amendement écarte les « témoignages contre soi-même ». Le quatorzième amendement garantit la liberté d'opinion en matière de mariage et d'éducation.

Dans certains Etats[220], le droit à la vie privée a été proclamé et a une valeur constitutionnelle. La Californie considère ainsi que le droit à la vie privée est un droit inaliénable[221].

L'Etat fédéral s'est doté en 1974 d'un Privacy Act. Cette loi encadre l'utilisation des données personnelles détenues par l'administration fédérale. Sont qualifiées de données personnelles les informations relatives à une personne physique, afférentes à l'éducation, aux transactions financières, à la santé, au casier judiciaire, à la profession, avec nom ou identifiant numérique, symbole ou tout autre identifiant propre au sujet, tel qu'un échantillon de l'empreinte digitale, de la voix ou sa photographie[222].Les données biométriques sont expressément incluses parmi les données personnelles. Cela englobe le gabarit de l'iris, de la rétine ainsi que les échantillons de sang ou d'ADN. Le privacy Act ne concerne évidemment pas le secteur privé. Lorsqu'une personne physique subit un préjudice de la part d'une société qui a vendu des informations la concernant, seul le droit de la responsabilité peut être invoqué.

Depuis les attentats du 11 septembre et l'institution d'une politique ultra sécuritaire, la biométrie s'est particulièrement développée.

I) Le contrôle des flux migratoires

A) L'amélioration de la prise en charge des passagers

---

[218] CIC

[219] ADRC

[220] La Californie

[221] Constitution de l'état de Californie, article un, Declaration of Rights section 1 : « All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing and protecting ptoperty, and pursuing and obtaining safety, happiness, and privacy »

[222] U.S.C& 552 a (a) (4) Record means « any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, fiancial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol,or other identifying particular assigned to the individual suchs a finger or voice print or a photograph"

Dès 1993, les autorités américaines chargées de l'immigration ont mis en œuvre à l'aéroport de New York un dispositif dénommé FAST (Future automated screening for travellers). Ce dispositif permettait l'identification des passagers. Il faisait suite au projet INSPASS (Immigration and naturalisation service passenger accelerated service system). L'objectif était d'améliorer la prise en charge des passagers. Les voyageurs volontaires donnaient, lors de l'enregistrement, leur identité et le gabarit de la paume de la main. S'il n'était pas possible de recourir à la reconnaissance palmaire, les empreintes digitales étaient utilisées. Le gabarit est enregistré sur une carte dont le contenu est mis à jour chaque année. Les voyageurs engagés dans ce programme étaient pour l'essentiel des ressortissants américains et canadiens, et, dans une moindre mesure, les ressortissants des pays signataires d'un accord de dérogation de visa[223]. Il était prévu d'introduire le projet dans 23 aéroports situés au Nord de l'Amérique.[224]Il y avait en 1999 près de 45000 personnes[225] enregistrées dans la base de données du service d'immigration américain passant en moyenne quatre fois par an aux bornes INSPASS[226]. INSPASS était également une réponse à la lutte contre les substitutions de personnes.

B)Le contrôle de l'immigration :

La biométrie a aussi été utilisée pour contrôler l'immigration. En 1940, a été adoptée une loi visant à réguler l'entrée des étrangers. Cette loi disposait que tous les étrangers entrant aux USA devaient se faire enregistrer[227] avec leurs empreintes digitales. L'enregistrement était réalisé en double exemplaire, l'un à destination du consul, l'autre à destination des autorités américaines (visa), qui transmettaient le dossier aux services de l'immigration, pour examen, puis au ministre de la justice. Les mineurs de moins de quatorze ans n'étaient pas soumis à cette obligation. L'Illegal Immigration reforme and immigrant responsibility Act de 1996 généralise cette formalité par l'introduction d'un système automatique de contrôle des entrées et sorties sur le territoire américain afin d'identifier les personnes qui restent au-delà du délai prescrit[228]. L'Immigration and nationality Act[229] applique la procédure d'enregistrement de l'Alien Registration Act de 1940 aux étrangers de plus de quatorze ans demeurant aux USA depuis plus de trente jours. Le dépôt d'un gabarit d'empreinte digitale est obligatoire pour tous les demandeurs de visas. La section 326 de la loi invite le Commissaire de l'immigration et de la naturalisation à développer un système d'identification des criminels étrangers afin de leur interdire l'entrée sur le territoire américain et faciliter les recherches policières.

Des expériences récentes recourent à la reconnaissance faciale. Ce changement s'inscrit dans les directives de l'Organisation internationale de l'aviation civile.

C) Le contrôle de l'identité des passagers

La politique du gouvernement américain consiste à interdire l'accès du territoire aux éventuels « terroristes ». Il s'agit de contrôler l'immigration en renforçant la procédure d'octroi de visas. Le Patriot Act de 2001 étend les pouvoirs du gouvernement en matière de surveillance, facilite le contrôle de l'entrée et de la sortie des étrangers, utilise la biométrie dans la délivrance des visas : ces dispositions sont explicitées dans le Enhancer Border Security and Visa Entry Reform Act de 2001. Il est prévu et de

[223] Cet arrangement permet aux voyageurs restant moins de 90 jours aux USA de ne pas solliciter de visa. Sont concernés le Royaume-Uni, l'Australie, la Nouvelle-Zélande.

[224] Peuvent être cités les aéroports de Seattle, Washington, Honolulu, Hawai, Atlanta, Boston, Chicago, Cincinnati, Dallas, Détroit, Houston, Minneapolis, Montreal, Orlando, Ottawa, Saint Louis.

[225] John.D. Woodward,Jr « Biometrics,Facing up to terrorism »octobre 2001, Rand Arroyo Center

[226] http://www.bcis.gov

[227] Alien registration Act, 1940

[228] Section 101

[229] Section 262

renforcer les applications d'INSPASS. Selon la section 403 paragraphe c du Patriot Act, le ministère de la justice et le ministère des affaires intérieures doivent travailler, avec le concours du National Institute of Standards and Technology, à l'élaboration de technologies utilisées pour identifier les demandeurs de visas et les personnes pénétrant sur le territoire américain. La technologie choisie doit être identique dans toutes les administrations pour faciliter les échanges. Les administrations fédérales qui ont à connaître des questions de l'immigration sont invitées à mettre en œuvre les meilleurs moyens techniques pour contrôler l'immigration et assurer la sécurité des frontières. La section 405 dispose que le ministre de la justice doit faire un rapport au Congrès sur le système d'empreinte digitale du FBI. Ce rapport fait également le bilan sur les systèmes qui sont utilisés dans les autres administrations fédérales. Selon la section 414 du Patriot Act, des mécanismes d'identification sont mis en place non seulement dans les aéroports, mais aussi dans les ports et à tous les points d'entrée du territoire américain. Par ailleurs, le Patriot Act préconise l'utilisation de techniques biométriques et d'autres moyens rendant infalsifiables les documents d'identité[230]. Un passeport biométrique authentifie l'identité des citoyens qui voyagent à l'étranger. Le document est bien sécurisé, mais onéreux. Il contient un circuit intégré où sont transcrits la photographie du détenteur du passeport et des renseignements d'ordre biographique. Le coût de cette politique sécuritaire est élevé dans la mesure où sont nécessairement fabriqués des instruments destinés à la lecture des documents intégrant des données biométriques[231]. Les frais sont également supportés par les Etats étrangers. Les pays qui participent à l'US Visa Waiver Program doivent mettre en place des machines capables de lire les passeports. La généralisation des passeports biométriques est prévue pour octobre 2004.Cette date butoir sera peut-être repoussée : tous les pays de l'US Visa Waiver Program ne sont pas prêts. Par ailleurs, la reconnaissance faciale a montré ses limites aux USA, terre d'élection. Les aéroports de Floride et de Boston ont abandonné cette technologie qui générait un nombre important de faux résultats.

Enfin, le Pentagone envisage de déployer un programme pour combattre le terrorisme, « Terrorist Information Awareness (TIA) program ». Il s'agit d'installer une base de données contenant des informations médicales, financières, des interceptions de correspondances, des données biométriques sur les présumés terroristes. Le Congrès a demandé au Pentagone de préciser l'objet du programme[232].

II/ La lutte contre la délinquance et la criminalité : A) la reconnaissance faciale a été utilisée pour faire diminuer la délinquance. De nombreuses villes, telle Tampa en Floride, ont fait appel à la société Visionics, spécialisée dans l'installation de caméras video[233]. La police de Tampa a notamment utilisé la reconnaissance faciale lors du 35ème Super Bowl en janvier 2001. Quelques délinquants ont été identifiés[234] mais aucun n'a été arrêté.

Aux USA, et malgré une relative inefficacité, la reconnaissance faciale est préférée aux autres techniques biométriques : elle ne porte pas atteinte à l'intégrité physique et elle n'induit pas d'effets psychologiques délétères. La reconnaissance palmaire répugne à

---

[230] Development of the system. In the development of the integrated entry and exit data system under section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (U.S.C 1365 a), the Attorney General and the Secretary of State shall particularly focus on

1) the utilization of biometric technology
2) the development of tamper resistant documents readable at ports of entry

[231] L'introduction d'une carte d'identité nationale est impossible tant elle a soulevé de tollé chez les conservateurs et chez les défenseurs des droits de l'homme.

[232] http://www.aclu.org

[233] Il y aurait à New York 1200 caméras de surveillance visibles.

[234] des pickpockets

certaines personnes pour des raisons de prophylaxie. L'hygiène intervient aussi pour l'iris et la rétine. Les empreintes digitales ne sont pas intrusives mais contiennent un stigma et leur image est liée à la criminalité. De plus, les empreintes digitales étaient utilisées pour contrôler les mouvements de population. Elles ont permis, notamment de contrôler les minorités ethniques, noires et asiatiques. Sur le fondement de cette discrimination, les autorités ont favorisé les préjugés racistes, non sans conséquence pour la société américaine[235]. La reconnaissance faciale est en outre mieux acceptée par les communautés religieuses. Certaines sectes sont très opposées aux techniques biométriques.

B) L'accès aux lieux sensibles : 1) le sport : le super Bowl n'est pas la seule manifestation sportive qui s'est organisée sous contrôle biométrique. En 1996, lors des jeux olympiques d'Atlanta, l'accès au village olympique était soumis à la reconnaissance palmaire[236]. L'objectif était de prévenir les infractions en interdisant l'accès.

3) Les transports : la section 1008 du Patriot Act de 2001 prévoit d'implémenter la biométrie pour protéger les intérêts de l'Etat américain. Une étude est menée en collaboration par l'Attorney general, le ministre des transports concernant le recours aux identifiants biométriques, pour l'accès aux bases de données du FBI et des sites sensibles de l'Administration.

   En 2001, l'Aviation and transportation security Act promeut le recours à la biométrie dans les zones sensibles des aéroports.

   Comme l'immigration et la piraterie sont possibles par voie maritime, le Maritime transportation Act de 2002 stipule que les pilotes de navires et les personnes qui ont accès à des zones sécurisées dans les navires font l'objet d'une vérification d'identité et reçoivent un identifiant biométrique.

   Le département de la défense utilise la biométrie pour l'accès à ses sites sensibles et à ses bases de données. La technique usitée est la numérisation de l'empreinte digitale[237]. L'Armée collabore avec le Department's biometrics Management Office.[238]

   Le contrôle de l'accès permet de vérifier l'identité des personnes physiques et d'éviter les vols de papiers. Conscient de cet enjeu, le législateur américain projette de faire adopter une loi de modernisation des permis de conduire qui intégrerait des données biométriques[239].Les états de Georgie, Californie, d'Hawaii, de Floride envisageaient de réclamer le dépôt d'empreintes digitales pour la présentation à l'examen de permis de conduire[240].L'Illegal Immigration Reform & Immigrant Responsibility Act allait jusqu'à faire dépendre l'allocation d'avantages sociaux de la présentation d'un document d'identité[241]. Le projet a été suspendu : il était trop contraignant et trop coûteux.

   Après le 11 septembre, l'American Association of Motor Vehicle Administrators propose de participer à l'évolution des permis de conduire par l'introduction

---

[235] Cf en ce sens, Richard Sobel « The Demeanig of identification and personhood in national identification systems ». Cet auteur fait référence à Simon A.Cole « Suspect identities : a history of fingerprinting and criminal identification « (2001)

[236] www.recogsys.com

[237] http://www.defenselink.mil/nii/biometrics/about/frameset.htm

[238] Par ailleurs, une loi de l'état de New York relative aux services financiers, le Financial Services fingerprinting Act de 2002 oblige les consultants et les employés d'une entreprise boursière à s'identifier avec leurs empreintes digitales..

[239] Driver license Modernisation Act 2002

[240] Ces projets de lois n'ont pas tous abouti.

[241] Ce document devait faire état du numéro de sécurité sociale.

d'empreintes digitales[242].Ce nouveau permis de conduire aurait à terme été utilisé comme carte nationale d'identité infalsifiable ; c'est ainsi que le législateur a présenté le Drivers license Modernisation Act.
Pour éviter les risques d'usurpation d'identité, le groupe Visa International travaille en partenariat avec un développeur de logiciel en reconnaissance vocale[243]. Les deux sociétés envisagent d'utiliser la biométrie pour sécuriser les transactions électroniques, le commerce « mobile » et « les risques de management ». Pour le moment, les expérimentations sont menées en interne parmi les employés de visa International[244]Les empreintes génétiques sont également utilisées.
Le FBI détient une base de données d'échantillons d'ADN des criminels. Le DNA Analysis Backlog Elimination Act de 2000 permet aux Etats d'effectuer des collectes d'échantillons, qui sont comparées à la base de données du FBI. Citons parmi les infractions retenues les homicides volontaires, les crimes sexuels, les enlèvements d'enfants, les cambriolages, les incendies criminels[245], certaines infractions commises par les militaires, les actes de terrorisme (Patriot Act). Le refus de se soumettre à un prélèvement d'échantillon constitue un délit. La biométrie a également été introduite dans les prisons non plus seulement pour tenir un registre de la population carcérale, mais encore pour contrôler les entrées et les sorties des prévenus et des visiteurs. Pour empêcher les substitutions de détenus, il est fait recours à la reconnaissance palmaire ou faciale.

C) L'accès aux soins : en 1996, la Health Insurance Portability & Accountability Act (HIPAA) a été adoptée afin de faciliter le transfert de l'assurance maladie en cas de changement d'employeur. L'HIPAA développait un identifiant médical unique. Les informations relatives au patient devaient être enregistrées dans un système électronique et dans une carte électronique contenant des données biométriques. Le projet n'a pas abouti. Un autre projet a été initié pour organiser la fourniture de médicaments grâce à une carte nominale. Ce projet est mis en œuvre progressivement ; il se heurte à la désapprobation des associations de droits de l'homme, hostiles à une carte d'assuré biométrique.[246]Aux USA, l'identification la plus usitée correspond au numéro de sécurité sociale que contiendrait la carte d'assurée biométrique. La présentation d'une telle carte pour accéder à des services pourrait aboutir à des discriminations. Ainsi, un employeur pourrait refuser une embauche à un candidat en mauvaise santé[247]. Les études ont démontré que les immigrés présentaient fréquemment un état de santé déficient. L'insertion sociale risque d'être plus difficile au vu des dispositions sécuritaires et biométriques.

III/ Les techniques biométriques et la loi. La réflexion est axée sur la reconnaissance facia le qui est souvent utilisée. Cette référence est riche d'enseignements.
La reconnaissance faciale porte-t-elle atteinte à la vie privée ?

A) La biométrie et le quatrième amendement : le quatrième amendement de la Constitution américaine garantit au citoyen le droit à la sûreté, à la non-violation du domicile, des papiers, des biens par des perquisitions et saisies arbitraires effectuées sans mandat.

---

[242] http://www.epic.org/privacy/id
[243] Vocent Solutions
[244] http://pcworld.co.nz « Visa gets behind voice recognition » Paul Roberts
[245] http://www.feds.com/basicsvc/public law/106-546.htm
[246] http://www.familieusa.org
[247] En France, une telle discrimination est prohibée. Seule, l'incompatibilité de la santé avec le poste à pourvoir peut justifier un refus d'embauche.

Appliquée à la reconnaissance faciale, il apparaît que cette technique est utilisée sans « mandat » de recherche. Les défenseurs des libertés publiques se sont vivement opposés à l'utilisation de la reconnaissance faciale lors du 35ème Super Bowl. En effet, les recherches ne doivent être diligentées par la police que s'il existe des suspicions fondées afférentes à la commission d'un crime. Les autorités ont fait valoir que cette technologie permettait de combattre la délinquance et n'avait aucune connotation raciste puisqu'elle ne procède à aucune discrimination. Les caméras étaient installées dans des lieux publics, et non privés. Enfin, dans certains cas limitativement énumérés, la loi permet des recherches sans mandat.

Existe-t-il un problème de constitutionnalité lorsque cette technique est utilisée dans les enquêtes criminelles pour mener à bien des investigations sur les lieux d'un crime ? Si les autorités utilisent la reconnaissance faciale comme technique d'investigation, sans mandat, il faut que la situation soit en adéquation avec la jurisprudence Katz[248].

1) La prétention raisonnable à la vie privée : Katz c/ Gouvernement des Etats-Unis

a) Pour que l'activité de la police constitue une enquête, il faut que la personne ait exprimé une prétention à la vie privée[249]et que cette attente personnelle[250]soit socialement raisonnable. Le quatrième amendement protège le droit à la vie privée dans la sphère intime et non dans la sphère publique. En procédant par analogie dans le domaine de la biométrie, les citoyens ne peuvent exiger la protection de la voix, du visage, de la signature, de la démarche. Dans l'arrêt United States v. Dionisio, le jury souhaitait obtenir un échantillon de voix afin de le comparer avec des conversations enregistrée figurant parmi les éléments de preuve. La Cour décide que « les caractéristiques physiques vocales d'une personne telles que sa voix et sa manière de parler, contrairement au contenu d'une conversation, sont exposées au public »[251]

   En revanche, les empreintes génétiques, le sang, la salive ne sont pas « exposés au public » et leurs caractéristiques sont protégées par le quatrième amendement. L'accès à ces données n'est possible qu'en portant atteinte à l'intégrité physique du corps. La Cour suprême a jugé que lorsque le déroulement d'une enquête impose l'atteinte à l'intégrité physique de l'individu, un mandat est nécessaire. A défaut, il y a violation du quatrième amendement[252]. De même, les données doivent avoir été obtenues lors d'une détention légale. La Cour Suprême valide des écoutes clandestines en arguant qu'il n'y avait pas violation de l'intégrité physique[253]. Avec la reconnaissance faciale, l'image obtenue n'est ni le résultat d'une détention illégale, ni l'objet d'une atteinte à l'intégrité physique. Alexander T Nguyen critique les dérives possibles. L'individu qui est soumis à une analyse vocale ou biologique s'est vu demander son consentement, alors que le consentement des personnes qui sont surveillées dans les lieux publics par le biais d'une caméra n'est pas recueilli. Sans tenir compte du degré d'intrusion, une enquête porte toujours atteinte à la dignité d'une personne. Quant à la reconnaissance faciale, elle peut être perçue comme intrusive puisqu'elle porte atteinte à la dignité des individus comme le ferait une enquête.

---

[248] Katz v United States 389 US 347 1967
[249] have exhibited an actual expectation of privacy
[250] donc subjective
[251] 410 U.S.1,14 (1973)
[252] U.S. v Dionisio
[253] Affaire Katz

b) Il faut également tenir compte du lieu de l'enquête. Il convient de limiter les intrusions dans la vie privée à l'occasion d'investigations policières. Lorsqu'une enquête implique une immixtion dans l'intimité de la vie privée, il faut obtenir un mandat ; en revanche, lorsque l'enquête n'implique pas d'immixtion dans l'intimité de la sphère privée, le mandat n'est pas nécessaire.
Le concept « public » a donné lieu à controverses. Les personnes physiques ne peuvent espérer la protection de leur vie privée pour les activités « publiques ». Cependant, dans l'arrêt Dow Chemical, la Cour suprême estime que la prise aérienne de photos d'une culture de marijuana sur la propriété d'un particulier n'est pas contraire au quatrième amendement[254] : pourtant la culture n'est pas accessible au public puisqu'elle est clandestine.
Alexander T Nguyen[255]compare la technique de reconnaissance faciale à la surveillance d'un lieu public par un policier qui mène une filature.

2) L'accessibilité des dispositifs : « general public use » : La Cour suprême a fixé des critères de conformité des dispositifs utilisés durant l'enquête.
   a) Lorsque le moyen utilisé est accessible au public, il n'est pas nécessaire d'obtenir un mandat. En revanche, si les services de police ont recours à des techniques sophistiquées, un mandat de recherche sera requis.
   La reconnaissance faciale, combinée au logiciel Facelt, est très connue dans le public. Le système est peu onéreux. Selon Alexander T Nguyen, la reconnaissance faciale est « general public use ».
   On ne peut qu'extrapoler sur l'iris et la rétine ; néanmoins, l'implémentation de la reconnaissance rétinale ou iridiale semble à la portée de tous.
   b) Les dispositifs plus complexes d'investigation requièrent un mandat : ils permettent d'offrir une capacité sensorielle que l'on ne possède pas. Sont conformes au quatrième amendement, peuvent être utilisés sans mandat les appareils qui permettent d'améliorer l'acuité visuelle, les techniques de détection à infrarouge, les jumelles, les télescopes. Est contraire au quatrième amendement une imagerie thermale utilisée sans mandat pour détecter une culture de marijuana.
   Les appareils de détection de métaux dans les aéroports, le recours à des chiens policiers sont conformes au quatrième amendement : les bagages ne sont pas ouverts.
3) Les enquêtes sont raisonnables[256]
   Il doit exister une présomption d'infraction. Un événement public comme le Super Bowl facilite la commission d'infractions. La numérisation d'un visage en vue d'une comparaison ne débouche pas obligatoirement sur une recherche intrusive. Cependant, une surveillance généralisée crée un climat de suspicion.
   Par ailleurs, les policiers peuvent détourner le dispositif de son objectif initial[257]. Dans ce cas, il n'y a plus de recherche raisonnable.

La recherche doit par ailleurs être circonscrite à un lieu. Or, si les caméras de surveillance sont installées dans une ville entière, l'ampleur du champ d'investigation peut faire perdre à l'enquête sa légitimité. Cependant, la jurisprudence n'est pas défavorable aux techniques biométriques. Dans l'affaire Davis c/ Mississipi, la Cour a

[254] Dow Chemical Co. V. US 476 US 227 (1986) et California v. Ciraolo 476 US 207 (1986)
[255] Here's Looking at you, Kid : has face-recognition technology completely outflanked the Fouth Amendment ? Virginia Journal of Law and Technology spring 2002
[256] « reasonable »
[257] Pour le profilage, par exemple.

stipulé que le recours aux empreintes digitales n'induit pas de disproportion comme pourrait le faire une enquête policière ou un interrogatoire.

B) La biométrie et le cinquième amendement : le cinquième amendement dispose que « Nul ne sera tenu de répondre d'un crime capital ou infamant sans un acte de mise en accusation (…) nul ne pourra, dans une affaire criminelle, être obligé de s'auto-accuser ».
Dans une étude menée par David McCormack, ce dernier confronte la reconnaissance faciale au cinquième amendement[258]. Il raisonne par analogie avec d'autres précédents jurisprudentiels. Dans l'affaire Gilbert c/California[259], la Cour a conclu que l'emploi d'échantillons manuscrits pour identifier des suspects ne viole pas le droit du défendeur visé dans le cinquième amendement.
Dans une autre affaire[260], la Cour précise que des échantillons de voix utilisés en vue d'une comparaison avec un enregistrement de conversations ne violent pas le cinquième amendement. Le juge rapporteur qui représente la majorité explique que l'exposition des caractères physiques identifiables ne viole pas l'interdiction de l'autoaccusation[261].
Selon David MacCormack, il importe peu que la reconnaissance faciale soit actuellement utilisée par le biais d'un affichage des caractéristiques physiques qui ont été compilées, même si cela a été fait sous la contrainte, puisque la Cour suprême estime que cette compilation de données est conforme au droit. La loi prévoit l'utilisation du logiciel uniquement comme moyen d'identification des criminels ou des suspects. La reconnaissance faciale ne peut servir de preuve testimoniale pour établir la culpabilité de quelqu'un. Elle ne peut être assimilée à un témoignage de culpabilité dans la mesure où le système de correspondance alerte les autorités de la présence d'un sujet dont l'identité est contenue dans une base de données sur un lieu public, sans établir la culpabilité ou l'innocence de quelqu'un. Certains arguent que la jurisprudence concerne des hypothèses où des suspicions sont dirigées contre une personne, ce qui ne correspond en rien à la reconnaissance faciale dans les lieux publics. David MacCormack rejette cet argument. D'après lui, la reconnaissance faciale affecte les droits protégés par le cinquième amendement si le logiciel établit un lien entre une personne filmée dans la foule et le contenu de la base de données. Si le système identifie une personne physique, c'est parce que son signalement est contenu dans la base de données en raison de précédentes activités illégales. Les présomptions sont dirigées contre cette personne en particulier.

C) Le Privacy Act de 1974 : cette loi organise la collecte des données par l'administration fédérale et les autorités administratives indépendantes. Elle garantit le droit d'accès, le droit de procéder à des rectifications, le droit d'engager la responsabilité du gouvernement en cas de violation du Privacy Act. Cette responsabilité est engagée même lorsque l'administration ouvre ses registres à des tiers sans habilitation.
La collecte des données a lieu directement auprès du titulaire. Elle est nécessaire à la finalité poursuivie par l'administration. Elle ne doit pas révéler les opinions politiques des individus. Sur ce point, le Privacy Act rejoint les « données sensibles » du droit de

[258] David McCormack « Can Corporate America Secure our Nation ? An analysis of the Identix framework for the regulation and use of facial recognition technology »
[259] 388 US 263 (1967)
[260] United States v Dionisio 410 US 1 (1973)
[261] « It has been held that the compelled display of identifiable physical charecteristics infringes no interest protected by the privilege against self-incrimination »

l'Union européenne : il est hors de question de violer le premier amendement de la Constitution.

Pour que le Privacy Act s'applique aux fichiers des organismes fédéraux, les dits fichiers répondent à certains critères de classement. La tenue du fichier révèle des informations afférentes à l'identité des personnes fichées. Le classement est souvent nominatif, avec un numéro de sécurité sociale ou tout autre identifiant personnel.

Les droits de l'administré souffrent des exceptions. Le droit d'accès aux fichiers de l'administration ne s'applique pas dans un certain nombre de cas.[262] Par exemple, les fichiers relatifs à la sécurité nationale, ou les fichiers d'investigations policières ne sont pas accessibles[263]. Le droit d'accès n'est pas licite quand les informations collectées ont une origine confidentielle : il en est ainsi lorsque la police mène l'enquête et que des informations lui sont communiquées par une personne qui souhaite garder l'anonymat.

L'exception la plus intéressante[264] est l'exception d'utilisation ordinaire.. Elle permet le transfert de données en rapport avec la finalité poursuivie par l'administration. Il était prévu d'instituer une liste d'exceptions fondées sur l'usage ordinaire afin d'établir une distinction claire entre les transferts ordinaires d'informations et les transferts qui résultent d'une interprétation de la loi. Cette liste n'a jamais été publiée, alors que l'Office of Management and Budget devait veiller à une parfaite application de la loi.[265] Cette exception a induit de nombreux transferts de données entre administrations. Le législateur a tenté de contenir ces dérives par le Computer Matching and Privacy Act de 1988. Ce texte encadre le transfert de données ; les administrations peuvent refuser de transférer leurs données quand les exigences légales, selon elles, ne sont pas réunies. Les administrations qui échangent des données de manière habituelle pour compléter leurs fichiers sont tenues de soumettre ces transferts à une commission de vérification.

Le Privacy Act offre une protection très inférieure à celles dont bénéficient les citoyens européens. Il n'existe aucun organisme de régulation. L'Office of Management se charge seulement de la publication de lignes directrices. Le Privacy Act a été une réponse à la dissémination des données détenues par l'administration. Cette dernière s'est tournée vers le secteur privé. En matière d'immigration, les fichiers sont complétés par l'intermédiaire de personnes privées. En effet, la loi sur l'immigration demandait aux employeurs de salariés étrangers une vérification : les employés avaient-ils ou non procédé à l'enregistrement de leurs empreintes digitales lors de leur entrée sur le territoire ? Cette disposition a été contestée par les associations de défense des droits de l'homme mais elle est entrée en vigueur.

D) La législation des Etats fédérés : certains Etats ont légiféré en matière de biométrie.

1) Le New Jersey : le Biometric Identifier Privacy Act[266] de 2002 établit des recommandations pour l'utilisation des données biométriques. La loi prohibe la vente ou le transfert de données biométriques sans le consentement des personnes physiques. Les données biométriques détenues par des personnes privées sont conservées dans des conditions de sécurité satisfaisante.

---

[262] Dix

[263] De même que le fichier d'échantillons d'ADN du FBI

[264] Elle porte atteinte aux droits des citoyens

[265] Le Privacy Act de 1974 sous-section V confie à l'Office of Management and Budget le soin d'édicter des lignes directrices.

[266] www.njleg.state.nj.us

2) Le Texas : a adopté la Biometrics identifiers & voiceprint 2001. Comme dans le New Jersey, cette loi prohibe la vente ou le transfert des données biométriques sans le consentement des personnes physiques. Les données biométriques détenues par des personnes privées sont conservées dans des conditions de sécurité satisfaisante.
3) Etats fédérés/ Etat fédéral : au niveau des Etats, la définition de la biométrie n'inclut généralement pas l'ADN. L'ADN est cependant un identifiant biométrique, considéré comme tel par l'Etat fédéral[267].

   D'une façon générale, le point de vue des Etats fédérés et de l'Etat fédéral n'est pas toujours identique. Ainsi, face aux dérives sécuritaires de l'Etat fédéral consécutives au Patriot Act, certains états fédérés, certaines communes ont adopté des législations plus libérales. Ces résolutions garantissent le respect des libertés fondamentales, encadrent les pouvoirs d'investigation de la police, rappellent l'importance des règles de procédure. Il s'agit surtout de limiter les interceptions de télécommunication illicites, le détournement de méls.

   Bien que la reconnaissance faciale soit considérée comme conforme à la Constitution, un état fédéré estime parfois que cette technique constitue une forme de profilage contraire au droit. Ainsi, la Californie restreint les applications de la reconnaissance faciale[268] Un projet de loi vise à encadrer son utilisation. La reconnaissance faciale a été définie par le Sénat californien comme l'utilisation de l'image d'un visage enregistrée à l'aide d'une caméra ou d'un autre moyen de prise de vue, combinée à un système permettant l'enregistrement et la transcription de l'image ou la relation entre des données du visage en une formule mathématique dénommée empreinte faciale, en vue de son enregistrement et de sa comparaison avec d'autres données ou photographies afin d'identifier une personne. Le projet de loi dispose qu'il est interdit de créer une base de données biométrique sur des personnes innocentes, ou du moins non convaincues de crimes ou de délits. Les autorités ne pourront recourir à la biométrie que s'ils ne peuvent identifier les personnes physiques avec les moyens existants. La présence de caméras devra être signalée. Toute utilisation de techniques biométriques non conformes à la loi sera passible d'amendes.

   Dans sa version originale, le projet de loi exigeait que le recours à la reconnaissance faciale soit soumis à l'obtention d'un mandat. L'exigence a paru trop contraignante. Il eut été impossible de filmer une foule puisque la caméra aurait saisi l'image de personnes qui n'étaient pas mentionnées par le mandat.. Dans ce contexte, la reconnaissance faciale n'aurait pu servir qu'à contrôler un lieu précis, afin de surveiller des personnes préalablement identifiées. Cette version du projet de loi n'a donc pas été retenue par le sénat. Le lobby de l'industrie biométrique a fait ralentir l'adoption de la loi qui est toujours en suspens[269].

   Le bilan aux USA :

   Les critiques :

[267] cf : fichier d'échantillons génétiques du FBI

[268] S.B 169, 2001 Leg.session 2001-2002. Paul Nicholls « Bill would regulate biometric identifiers » Interetnews 17 février 1998

[269] Julia Scheeres « Face scanners turn lens on selves » Wired news 31 juillet 2001 ; http://www.Wired.com/news/privacy/0.1848.45687.00 html

La reconnaissance faciale permet le profilage des personnes physiques, ce qui porte atteinte à la présomption d'innocence. Elle est aussi porteuse d'un climat de suspicion qui peut avoir des effets destructeurs sur le tissu social.
De nombreuses questions pratiques surgissent. Des moyens suffisants doivent être déployés pour éviter la dissémination des informations, leur conservation et leur destruction. Les données biométriques sont plus complexes que les mots de passe, mais peuvent quand même être volées : il faut en tenir compte lors de l'implémentation d'un système d'identification biométrique. D'autres risques sont afférents à des détournements de fonction (function creep), soit un détournement de finalité. Par exemple, les autorités policières peuvent, durant leurs investigations, surveiller les activités d'un opposant politique. La reconnaissance faciale est détournée de sa finalité première, la surveillance d'un lieu public en vue de la filature d'une personne physique. Même lorsque certaines techniques sont conformes à la Constitution, leur application à une vaste échelle pose des difficultés. Ce point a été soulevé concernant les chiens renifleurs dans l'affaire Place par un magistrat dissident. Selon ce magistrat, avant d'admettre la conformité d'une technique de surveillance, il faut d'abord vérifier qu'il n'y a pas atteinte à la vie privée d'une personne. Une technique qui vérifie uniquement la présence de marchandises de contrebande est moins intrusive qu'une technique susceptible de révéler la nature même d'une marchandise ou d'un produit. Dans cette optique, la Cour ne tient pas compte des circonstances dans lesquelles sont utilisées ces marchandises et ouvre la voie à des abus. En effet, il serait possible selon cette jurisprudence que les policiers circulent, accompagnés de leurs chiens renifleurs. Il serait possible de scanner tous les passants, ce qui est incompatible avec le quatrième amendement de la Constitution. La notion de suspicion raisonnable n'aurait plus de raison d'être.

Les arguments en faveur de la biométrie :
Certains intellectuels avancent que la biométrie et particulièrement la reconnaissance faciale protège la vie privée des personnes issues des minorités. La reconnaissance faciale a pour avantage de respecter le principe de non-discrimination raciale[270] : la recherche est orientée vers des personnes dont l'identité est connue des services de police et ne prend pas en compte le faciès.. Le logiciel effectue une reproduction du visage et effectue des comparaisons avec les autres fichiers contenus dans la base de données des personnes recherchées. Toute collecte de données sensibles, santé, tendance sexuelle, situation financière est exclue.
Les techniques biométriques remédient à certaines faiblesses humaines. L'identifiant biométrique est le meilleur moyen de pallier les pertes, les oublis, les vols de mots de passe. Il facilite le travail de l'administrateur chargé de la sécurité qui n'est plus obligé de changer périodiquement les mots de passe.
Les risques d'atteinte à la vie privée sont minimes si l'organisme de collecte obéit à certaines règles de conduite. Ainsi, les données inutiles sont généralement détruites. En matière de reconnaissance faciale, lorsque les images des personnes filmées ne figurent pas dans la base de données, elles ne sont pas conservées.

La normalisation joue également un rôle important. Le Patriot Act invite les administrations à opter pour le même système de lecture et d'enregistrement des données biométriques pour faciliter les échanges de données. Il faut qu'une

[270] Quinzième amendement de la Constitution.

interface soit possible avec la base de données du FBI et que des échanges soient possibles entre les administrations. Ainsi, la loi Enhanced Border Security and visa Entry Reform Act organise la création d'une liste de surveillance commune à toutes les administrations compétentes en matière d'immigration et d'un système informatique commun.

Les échanges de données personnelles pourront se faire au niveau international puisque tous les pays membres de l'OACI utiliseront à terme le même standard. Or, la protection de la vie privée suppose la consolidation des systèmes d'information[271]. La création d'une unique base de données renforce les pouvoirs de l'Etat à l'égard du citoyen.[272]

Le passeport biométrique basé sur la reconnaissance faciale ne sera sans doute pas introduit dans les délais fixés par le gouvernement américain. Dans un rapport du General accounting Office de juin 2003, des recommandations sont faites pour renforcer les échanges d'information entre les services.[273] Pour l'instant, la date d'intronisation du passeport biométrique américain a été fixée au 26 octobre 2004, avec, comme technique de reconnaissance, les empreintes digitales. Au demeurant, les USA souhaitent imposer l'usage des empreintes digitales dans l'établissement des visas qui seront présentés sur le territoire américain.

QUATRIEME MODELE : L'AUSTRALIE

L'Australie est un état fédéral. Certaines matières font l'objet d'un double niveau de législation. La protection de la vie privée est garantie par des lois fédérales et par des lois applicables dans les Etats fédérés. L'accent sera surtout mis sur la législation fédérale.

Le Privacy Act australien date de 1988. A l'origine, cette loi ne devait s'appliquer qu'aux collectes de données effectuées par des organismes étatiques. Les fichiers de données personnelles sont régis par les onze principes « Information privacy Principles » (IPPs).

Depuis lors, le Privacy Act a été révisé afin de prendre en compte les collectes de données effectuées par les organismes privés.[274]La nouvelle législation est entrée en vigueur le 21 décembre 2001. Elle soumet le secteur privé à des « National Privacy Principles » (NPPs). Ces derniers précisent comment s'effectue la collecte des données. La réforme institue un droit d'accès aux données personnelles. L'obligation d'information porte sur les modalités de collecte des données, sur la finalité, sur les personnes qui accèdent à ces informations.

Il est possible de substituer aux NPPs des codes de protection de la vie privée qui doivent être approuvés par le Privacy Commissioner. Ces codes instituent des procédures amiables de règlement des litiges. Ces codes permettent d'éviter les sanctions prévues par une loi exigeante et complexe tout en assurant aux personnes physiques un minimum de protection. Le Privacy Act de 1988 ne traite pas explicitement des données biométriques. La législation ne réfrène pas de manière

[271] Par leur sécurisation, leur mise à jour.

[272] Richard Sobel « The Demeaning of identity and personhood in national identification systems » Harvard Journal of Law & Technology Vol.15, n°2 spring 2002

[273] http://www.gao.gov/atext/d03798.txt

[274] Privacy Amendement Private sector Act 2000 Commonwealth

satisfaisante les intrusions dans la vie privée : le Privacy Act de 1988 comporte des imprécisions.

I) La préservation de la sécurité nationale par la biométrie

Comme dans la plupart des pays développés qui connaissent d'importants flux migratoires, l'Australie introduit la biométrie pour contrôler ses frontières. D'autres applications biométriques sont mises en œuvre afin de contrôler l'identité des personnes.

A) Le contrôle des flux migratoires et de la criminalité.

Dès janvier 2003, les douanes australiennes ont instauré un système de passeport biométrique. Ce système a été introduit avant l'expiration du délai d'expérimentation qui devait durer six mois.

Le système d'identification, dénommé Smartgate, repose sur la reconnaissance faciale de volontaires, qui, dans la majorité des cas, étaient des agents de compagnies aériennes.

Sur 6000 volontaires, le système a reconnu 80% des personnes enregistrées. C'est ce succès qui a justifié l'accélération de l'expérimentation publique. Des critiques se sont fait jour : des erreurs sont apparues en raison du mauvais enregistrement des photos ; Smartgate numérise le visage de chaque volontaire et le compare à une représentation de quatre photos. La formule est ensuite enregistrée dans le passeport.

A la suite de cette expérimentation, le gouvernement australien a décidé d'introduire en 2004 un passeport avec données biométriques. L'adoption du passeport biométrique est confortée par la décision de l'Organisation Internationale de l'aviation civile qui envisage de retenir la reconnaissance faciale comme standard universel pour la sécurité aérienne.[275]L'Australie a une expérimentation de deux ans, ce qui correspond à 6,5 millions de dollars d'investissement.

La biométrie permet de lutter contre la fraude en matière d'identité. L'Australie est un pays de forte immigration, qui génère un important trafic de pièces d'identité[276]Cela a justifié l'institution d'un répertoire de candidats à l'immigration avec données biométriques. Ainsi, le Migration Act de 1958 stipule que si une personne est placée en détention pour immigration illégale, les services de police doivent procéder à son identification.[277]. La technique la plus répandue est celle des empreintes digitales. La collecte des gabarits est encadrée par des instructions ministérielles[278]Les mineurs ne sont pas soumis au relevé des empreintes digitales. Le fichier et le gabarit doivent être détruits dès que la personne a obtenu un visa. Seul un officier habilité peut ordonner le relevé des empreintes digitales qui doit être effectué par une personne du même sexe que le prévenu, en présence d'un témoin. Un projet de loi en date du 26 juin 2003 doit réformer le Migration Act de 1958. Qualifié de « Migration Legislation Amendment (« Identification and Authentification »), le projet propose une définition des identifiants personnels, précise les modalités de délivrance, d'utilisation, de conservation, de destruction. Selon ce projet, sont considérés comme des identifiants personnels les empreintes digitales, la reconnaissance palmaire, la reconnaissance faciale, les indications sur la taille et le poids, les enregistrements audio et video, l'iris.

---

[275] Réaffirmation de cet engagement lors du sommet d'Evian réunissant le G8.

[276] En janvier 2000, 1508 personnes se sont vu refuser l'entrée dans les aéroports ; 4317 personnes sont entrées par bateau sur le territoire australien. Le coût de la fraude en documents d'identité s'élèverait à 4 milliards de dollars par an. http://www.immi.gov.au/facts/74unauthorised.htm

[277] Migration Act 1958 section 258

[278] Migration Series Instruction 125 on fingerprinting of detainees

Le ministre doit s'assurer que le procédé respecte l'intimité de la personne : l'identifiant correspond à une partie externe du corps , il s'inscrit dans une finalité poursuivie par la loi[279]. Le projet de loi envisage les divers cas où un étranger doit se soumettre à un contrôle d'identité : demande de visa, entrée en zone de contrôle d'immigration, suspicions relatives à l'irrégularité de la situation d'un individu au regard de l'immigration. Le projet rejette les procédés intrusifs : prélèvement de salive, de sang, de poils pubiens, échantillon buccal, examen des parties génitales. Aucune disposition n'est prévue concernant les échantillons d'ADN, qui ne doit pas être exclu pour autant. En effet, le Migration Act a déjà recours aux analyses génétiques : les tests d'ADN sont prévus pour établir un lien de parenté[280]et pour des raisons sanitaires à l'endroit des candidats à l'immigration. Le ministère à l'immigration et aux affaires multiculturelles indigènes[281]envisage l'utilisation de tests génétiques pour l'identification des demandeurs d'asile[282].
La future loi instaure des garanties procédurales. La collecte de gabarit se fait dans le respect de la vie privée. Les personnes arrêtées sont informées dans leur langue. Le projet établit une distinction entre les personnes physiques ne détenant pas la citoyenneté australienne et les personnes physiques ne détenant pas la citoyenneté australienne détenues en zone d'immigration. Pour cette dernière catégorie, il est possible de recourir à la force pour exécuter la procédure d'identification si la personne refuse de se livrer à ladite procédure. Un refus rend toute demande de visa invalide et fait naître des suspicions sur la situation[283]du candidat.
Pour les mineurs de moins de dix-huit ans, le consentement des parents ou du représentant légal est indispensable. Pour les mineurs de moins de quinze ans, la biométrie n'est pas utilisée.
A terme, les informations biométriques devront être supprimées. Des exceptions demeurent : détention en zone d'immigration, refus de la demande de visa, maintien sur le territoire national au-delà de la date d'expiration du visa temporaire.

B) La prévention du terrorisme

L'Organisation internationale de l'aviation civile s'est prononcée en faveur de l'utilisation de techniques biométriques à l'échelle mondiale pour lutter contre les actes de piraterie aérienne. L'Australie a adopté un Terrorism Act en 2002, malgré les protestations des défenseurs des droits de l'homme[284]et les réserves du Sénat. Durant les travaux parlementaires, une Commission d'enquête a souligné les dangers que présenterait ce texte pour les libertés publiques et s'est penchée sur les procédés biométriques dans les aéroports[285]. Le rapport du Federal Privacy Commissioner insiste sur la nécessaire proportionnalité entre la finalité poursuivie et les moyens utilisés. Un dispositif permettant de scanner le corps d'un individu afin de déterminer s'il possède des armes est disproportionnée, d'autant que d'autres méthodes moins intrusives permettent d'atteindre les mêmes résultats.

---

[279] Il s'agit de détecter le « forum shopping » pratiqué par les candidats à l'immigration
[280] regroupements familiaux
[281] Department of Immigration and Multicultural and Indigenous Affairs (DIMIA)
[282] Il convient de vérifier si les demandeurs d'asile ne se sont pas vus refuser la demande d'asile dans un autre pays.
[283] Est-elle régulière ?
[284] Cf : Roger Clarke « Biometrics in Airports. How to, and how not to, stop Mohammed Atta and Friends » février 2003 http://www.anu.edu.au./people/ Roger Clarke/DV/BioAirports.html
[285] Senate Legal and Constitutional Legislation Committee « Inquiry into Terrorism Bills » Submission from the Federal Privacy Commissioner april 2002

C) La délivrance de services

La biométrie permet d'identifier une personne et de s'assurer de ses qualités de manière fiable. Les risques d'usurpation d'identité sont diminués. En Australie, des systèmes de reconnaissance biométrique ont été institués pour parvenir à identifier les personnes prétendant à l'octroi de pensions ou à l'accès aux soins. Une expérience d'identification par l'iris a été réalisée au sein d'officines de pharmacie pour la délivrance de méthadone. Le système baptisé Methadose a réduit les risques de double délivrance du produit en effectuant une vingtaine de contrôles. L'intérêt du dispositif est surtout remarquable dans les grandes officines où le pharmacien ne connaît pas tous ses clients. Par ailleurs, les fichiers des patients sous traitement sont actualisés.[286]

II) Les sources du droit australien en matière de vie privée au regard de la biométrie

A) Le droit international : le Pacte international relatif aux droits civils et politiques.

L'Australie est signataire du Pacte international relatif aux droits civils et politiques du 16 décembre 1966. Son article 17 stipule que « nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée… ». Le Comité des droits de l'homme précise[287]que les législations nationales doivent garantir ce droit en empêchant les immixtions, notamment de la part des pouvoirs publics.

Le droit à la vie privée n'est cependant pas absolu. Le Comité des droits de l'homme prend en compte les exigences de la vie sociale. En conséquence, les immixtions doivent être encadrés par des dispositifs normatifs et indispensable à la vie sociale au sens du Pacte.

Le projet de loi réformant le Migration Act de 1985 sera analysé au regard de cet article 17. La politique de contrôle de l'immigration justifie-t-elle des collectes de données biométriques en violation du Pacte international ? Selon la réforme du Migration Act de 1958, la collecte des données prend des formes particulièrement intrusives et coercitives dans la mesure où les prévenus, candidats à l'immigration, peuvent faire l'objet de relevé de données biométriques alors même qu'ils ont opposé leur refus.

Le Pacte est peu contraignant. L'introduction de l'instance par un Etat rend illusoires les hypothèses de plaintes introduites devant le Comité[288].

B) Le Privacy Act de 1988 : il protège les données ayant un caractère personnel. Les données biométriques contiennent des informations relatives à un individu et permettent de l'identifier[289]. Le Privacy Act définit les données personnelles comme toute « information ou opinion (y compris celle contenue dans une base de données), qu'elle soit vraie ou fausse enregistrée sur support analogique ou non, relative à un individu dont l'identité est apparente ou qui peut facilement en être déduite ». L'article 16 du Privacy Act dispose que l'organisme de collecte ne peut pas rassembler et dévoiler de manière irréfléchie. La collecte de données doit être nécessaire à l'accomplissement d'une finalité légale en rapport avec l'activité de l'organisme. Dans le projet de loi destiné à amender le Migration Act de 1958, le but de la collecte de données biométriques concerne l'identification des personnes. Se pose alors la question de l'opportunité et de la proportionnalité de la

[286] Rachel Lebihan « Drug dispensing device demands an aye for an eye » daté du 19 juin 2003 in Australian Financial Review supplement, page 13, http://www.argus-solutions.com/afr19jun03.html

[287] Dans ses observations générales afférentes à l'article 17

[288] Article 41 du Pacte

[289] « Biometrics and Privacy the End of the World as we know it or the white knight of privacy »20 mars 2002

collecte des informations en prévision de fraudes potentielles à l'immigration ou d'usurpation d'identité par des personnes n'ayant pas la nationalité australienne.
Quant aux données génétiques, elles sont protégées par le Privacy Act de 1988. Les organismes publics et privés qui procèdent à ces analyses sont soumis respectivement aux IPPs et aux NPPs. Le consentement de la personne sera obtenu. Les données collectées ne peuvent être disséminées et dévoilées à des tiers non habilités. La collecte doit se faire dans le respect de l'intimité de la personne.
Ces garde-fous ne présentent pas de garanties suffisantes. Ainsi, le Disability Discrimination Act de 1992 permet des discriminations fondées sur le Migration Act de 1958.[290] Ces dispositions peuvent s'avérer lourdes de conséquences pour certaines demandes de visas et pour le regroupement familial. L'administration risque de refuser l'entrée du territoire à un étranger présentant des pathologies lourdes[291]. Par ailleurs, le projet de loi réformant le Migration Act de 1958 permet le prélèvement des données biométriques sans le consentement de la personne physique, si l'officier fait face à une opposition.[292]En effet, le Privacy Act prévoit que la collecte de données ne puisse être effectuée sans l'autorisation de l'individu mais cette prérogative n'a vocation à s'appliquer que lorsque les collectes sont effectuées par des organismes privés ; les données prélevées pour le compte d'un organisme étatique ne nécessitent pas l'autorisation du titulaire, en particulier en matière criminelle lorsque des prescriptions légales ou réglementaires l'imposent.
Le transfert des données à des tiers et leur commercialisation est interdit tant que le sujet n'a pas exprimé son consentement. Ce principe s'applique strictement aux organismes privés de collecte. En revanche, pour le secteur public, le Privacy Act de 1988 autorise la révélation d'informations à des tiers dans tous les cas où des dispositions législatives l'autorisent expressément. Le Migration Act de 1958 peut organiser le transfert de données biométriques entre des Etats qui ont mis en place une politique restrictive d'immigration. Le transfert de données à des tiers ne concerne pas les échanges entre les organismes étatiques qui ont convenu de coopérer ensemble à la mise en œuvre de la politique fédérale. Cette interprétation de la notion de transfert à des tiers favorise les dérives quant à l'utilisation des données. Les risques sont graves lorsqu'il s'agit de données génétiques. Au demeurant, les donnés génétiques peuvent être disséminés auprès d'organismes privés par des autorités peu scrupuleuses par exemple lors des tests en recherches de paternité.
Le Privacy Act ne traite pas des relations de travail. Il s'applique aux fichiers de données élaborés par les employeurs depuis la réforme de 2001 instituant les NPPs. Ces derniers s'appliquent entre particuliers ; les données biométriques relevées par un employeur sont soumises aux principes d'autorisation préalable, de contrôle, d'accès pour l'employé. Quant à la reconnaissance faciale, est-elle concernée par le Privacy Act ? Ce dernier ne fait pas allusion au contrôle des salariés sur le lieu de travail par le biais de la video-surveillance. Il convient de se référer aux règles du droit du travail pour obtenir des précisions à ce sujet. Or, seuls les Etats de la Nouvelle Galles du Sud et de Victoria ont adopté des législations spécifiques. La loi fédérale, le Workplace relations Act de 1996, traite de généralités.
La Nouvelle Galles du Sud a adopté en 1998 le Workplace Video Surveillance Act. Cette loi érige en délit l'utilisation de caméras dissimulées sur le lieu de

[290] Article 52 du Disability Discrimination Act de 1992
[291] Ex : le VIH
[292] cf : supra pour le seul cas des personnes arrêtées pour immigration clandestine

travail en dehors de quatre cas limitativement énumérés. L'installation de caméras de surveillance doit faire l'objet d'une notification écrite. Elle peut se faire à la demande d'un magistrat qui enquête sur un salarié.

L'Etat de Victoria a également une loi afférente à l'utilisation de caméras de surveillance, le Surveillance Devices Act qui a pris effet en janvier 2000. Son champ d'application concerne l'ensemble des activités privées et ne se limite pas aux lieux de travail.

En confrontant ces textes avec la reconnaissance faciale, il paraît évident qu'une telle technique ne pourrait être mise en œuvre à l'insu des salariés.

L'Australie est prête à accueillir la biométrie, mais en tenant compte d'un cadre juridique précis.

CINQUIEME MODELE : LA NOUVELLE ZELANDE

Comme l'Australie, la Nouvelle Zélande a adopté une loi relative à la protection des données personnelles sous l'impulsion des lignes directrices de l'OCDE. La loi est intervenue tardivement, en 1993. Le législateur néo-zélandais a été plus ambitieux que le législateur australien : il a analysé les différents systèmes juridiques existant dans d'autres pays et a organisé une protection assez complète. Le Privacy Act de 1993[293]s'appliquait dès l'origine aux relations entre particuliers. L'objectif du Commissioner néo-zélandais est d'aboutir à une législation aussi protectrice que les législations européenne et canadienne.[294]Le Privacy Act de 1993 précise que la collecte des données personnelles doit être nécessaire, avoir un lien avec l'activité de l'organisme qui procède à cette collecte. La collecte des données doit se faire directement auprès de la personne concernée qui est informée de l'existence et de la finalité de la collecte. Les données ne peuvent être collectées de manière illégale ou par un moyen intrusif.

Il n'existe en Nouvelle-Zélande aucune législation relative à la biométrie ni même, comme le regrette le Privacy Commissioner[295], de législation relative à la surveillance des personnes. Actuellement, seul le Privacy Act de 1993 peut être invoqué à l'encontre de la politique sécuritaire qui a été adoptée en Nouvelle-Zélande après le 11 septembre. Des systèmes biométriques de contrôle d'identité et de surveillance sont installés ou en expérimentation. Nicky Hager reproche à ces initiatives privées et publiques d'être sans commune mesure avec la réalité des menaces terroristes qui pourraient concerner la Nouvelle-Zélande. La préservation de l'intimité et de la vie privée est souvent sacrifiée. Seule l'adoption d'amendements ou de lois sectorielles pourrait combler les lacunes du Privacy Act. Un exposé des failles a été présenté par le professeur Paul Roth lors du Privacy Forum tenu en mars 2003 à Wellington.[296]Paul Roth relève le manque d'effectivité des dispositions législatives lorsqu'elles ont vocation à s'appliquer en droit du travail. Par ailleurs, le Privacy Act de 1993 ne s'applique pas aux données collectées clandestinement par le biais de caméras vidéo

[293] Ce qui n'est pas le cas dans la situation australienne

[294] Cf : commerce électronique. Voir également un rapport de la Law Commission de février 2002 « Protecting Personal Information from disclosure ». Cf aussi les recommandations faites au ministre des affaires étrangères concernant le projet de loi contre le terrorisme, s'inspirant de la doctrine du Privacy Commissioner canadien http://www.privacy.org.nz/people/countter2.html

[295] Rapport du Privacy Commissioner au ministre de la justice du 7 février 2003, afférent au projet de loi contre le terrorisme. Il s'agissait de propositions visant à l'encadrement des dispositifs permettant de pister les individus.

[296] Paul Roth « Reflections on ten years of the Privacy Act » consultable sur le site www.privacy.org.nz

ou par d'autres techniques. Dans un rapport du 20 janvier 2003, le Privacy Commissioner Bruce Slane recommande l'adoption d'un processus juridique garantissant l'utilisation de surveillance vidéo secrète.
La Nouvelle-Zélande est signataire du Pacte international relatif aux droits civils et politiques. Le Bill of Rigths réaffirme l'attachement de la Nouvelle-Zélande aux principes contenus dans le Pacte. L'un des articles du Bill of Rights Act rappelle que les droits et libertés proclamés ne peuvent être soumis qu'à des limites raisonnables fixées par la loi et indispensables au maintien d'une société démocratique.[297]

L'application du Privacy Act de 1993 à la biométrie : il convient de déterminer la qualification des données biométriques en tant que données personnelles au sens du Privacy Act de 1993. Le concept de données biométriques n'est pas contenu dans le Privacy Act de 1993. Néanmoins, il ressort des interventions du Privacy Commissioner que les données biométriques sont des données personnelles. La notion d'information personnelle s'entend d'une donnée concernant un individu identifiable. Les données biométriques répondent sans conteste à cette définition comme cela a été exposé pour le Privacy Act australien. A contrario, le Privacy Act ne peut être invoqué lorsque la personne n'est pas identifiable. Ainsi, l'installation de video-surveillance échappe aux dispositions législatives dès lors que les personnes filmées ne peuvent être individuellement reconnues. Cet aspect concerne notamment la reconnaissance faciale. En principe, les logiciels de reconnaissance faciale nécessitent plusieurs photographies qui sont traduites par des algorithmes. Ces derniers sont par la suite comparés avec le visage de la personne qui se présente devant les caméras. Cela implique que la personne concernée ait consenti à la prise des photos gabarit et qu'elle se soumette au contrôle. Cependant, les photos peuvent être prises à l'insu de la personne physique. Les techniques de reconnaissance faciale peuvent procéder à des contrôles d'identification quelle que soit l'allure à laquelle la personne passe devant la caméra.

I) Le contrôle de l'immigration

Les services des Douanes ont mis à l'essai en juillet 2002 un logiciel de reconnaissance faciale pour le contrôle des frontières. Ces expérimentations se sont étendues à d'autres services gouvernementaux, tel le ministère de l'immigration. Le service des douanes diligente une expérimentation en interne, qui s'applique ensuite aux équipages aériens. Le système sera placé sous la surveillance d'un officier des douanes pour pallier les éventuels dysfonctionnements du logiciel.
L'expérimentation de systèmes de reconnaissance faciale par le service des douanes s'inscrit dans le programme engagé par l'Organisation internationale de l'aviation civile afin de prévenir la piraterie aérienne. La Nouvelle-Zélande a adhéré à ce programme.
Par ailleurs, en application des recommandations de l'OACI, la loi américaine requiert qu'au 26 octobre 2004, les passeports des voyageurs se rendant aux USA contiennent un identifiant biométrique. Le journaliste Stephen Bell[298] émet des doutes sur l'installation immédiate de ce passeport en Nouvelle-Zélande. Il faut trouver et adopter un algorithme identique permettant d'enregistrer le gabarit pour assurer une bonne coopération internationale. Les décisions des services d'immigration risquent cependant de manquer d'impartialité et d'autonomie. Le refus de l'octroi d'asile ou de

[297] Bill of Rights 1990, Section 5 (justified limitations) : « Subject to Section 4 of this Bill of Rights, the rights and freedoms contained in this Bill of Rights may be subjected only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society »
[298] août 2003, computerworld.co.nz

visa par le département de l'immigration australien fondé sur les résultats de la base de données influencera sans doute les services néo-zélandais si le candidat se retourne vers la Nouvelle-Zélande.

II) Le droit du travail : le Privacy Act ne s'applique pas aux instances relatives au droit du travail ; la juridiction chargée de connaître les conflits du travail, Employment Court, s'est prononcée en ce sens en 1997. Le procès engagé par un salarié à l'encontre de son employeur ne peut être introduit que devant le Privacy Commissioner. Un débat s'est instauré sur la légalité des caméras video : en 1994, le Privacy Commissioner avait décidé dans l'affaire 0632 que de tels dispositifs n'étaient pas contraires à la loi ; par contre, en 2001, dans l'affaire 16479, le Privacy Commissioner a estimé que l'enregistrement des conversations d'un employé à son insu était contraire aux principes trois et quatre du Privacy Act : selon le troisième principe, lorsqu'une agence procède à des collectes d'informations auprès d'un individu, elle doit s'assurer que la personne est consciente qu'elle livre des informations personnelles ; le quatrième principe dispose que, pour la collecte des données, des moyens légaux équitables et non intrusifs doivent être mis en œuvre.

S'agit-il d'une évolution jurisprudentielle ? L'utilisation de dispositifs de surveillance par l'employeur doit être nécessaire à la découverte de comportements délictueux du salarié. Or, dans l'affaire 16479, il s'agissait d'un entretien disciplinaire et le salarié avait le droit de prendre connaissance de l'enregistrement. Aucune conclusion définitive ne peut être dégagée.

III) Le terrorisme et la criminalité

Le ministre de la justice a introduit en mars 2003 devant le Parlement un projet de loi anti-terrorisme. Ce dernier étend les pouvoirs de la police en matière de surveillance électronique.

Le Privacy Act de 1993 contient des garde fous contre la dissémination et le transfert de données personnelles. Le onzième principe encadre la communication des données personnelles à des tiers en listant des exceptions limitativement énumérées. Ainsi, les données ne peuvent être révélées à des tiers sauf si cela correspond à la finalité de la collecte. La révélation d'informations personnelles peut se justifier par le souci de la paix et de la sécurité publique. Par ailleurs, des lois organisent l'intervention du Privacy Commissioner.

C'est le cas avec le Passport Act de 1992. Les échanges de données entre le département des affaires internationales et le service des douanes doivent recevoir l'approbation du Privacy Commissioner, qui a été obtenue en 2001. Les échanges d'information entre le département néo-zélandais des affaires intérieures et le département australien des affaires multi-culturelles et indigènes doivent également être approuvées par le privacy Commissioner. Along terme, l'échange des informations concernera les données biométriques puisque la Nouvelle-Zélande participe au programme de l'OIAC.

Le Customs and Excise Act de 1996 exige que son responsable s'entretienne avec le Privacy Commissioner avant la signature de tout accord avec un organisme étranger qui procède à des transferts de données personnelles.

Après le Transnational Organised Crime Bill, l'Immmigration Act de 1987 a été amendé pour permettre la révélation de certaines données personnelles à des organisations étrangères. La révélation est licite pour le contrôle des frontières, la prise en charge des passagers en provenance de l'étranger. La consultation du Privacy Commissioner est exigée préalablement à la formalisation des accords de collaboration. En 2002, aucun accord de ce type n'avait encore été signé. La mise en

œuvre du programme de collaboration internationale pour octobre 2004 nécessitera sans doute de tels agréments.
L'Immigration Act permet à son directeur de dévoiler des informations à des organismes étrangers qui doivent faire respecter la loi ou qui sont en charge du contrôle des passagers et de la sécurité des frontières. Pour ces données spécifiques, l'approbation du Privacy Commissioner est recommandée.
Le Privacy Commissioner joue un rôle déterminant en Nouvelle-Zélande.

SIXIEME MODELE : L'AFRIQUE DU SUD

En Afrique du Sud, le droit à la vie privée est protégé par la coutume et par la Constitution.[299]Cependant, afin de s'adapter à l'importance croissante des transferts induits par la globalisation des relations commerciales et politiques, l'adoption d'une loi afférente à la protection de la vie privée est apparue nécessaire. Le Parlement travaille à l'élaboration d'une loi qui doit être votée fin 2003. Ce projet de loi s'inspire assez largement des directives européennes.[300]La loi définit la biométrie comme une technique d'identification personnelle basée sur les caractéristiques physiques qui incluent les empreintes digitales, la rétine et la reconnaissance vocale[301]. Les données personnelles sont des informations relatives à une personne identifiée ou identifiables grâce à un numéro, par un ou plusieurs facteurs afférents à son physique, sa physiologie, son état mental, sa situation financière, son identité culturelle ou sociale[302]. La définition légale doit être complétée par la notion d' « [303]information personnelle » proposée dans l'Electronic Communications and Transactions Act de 2002[304]. Dans ce texte qui organise le commerce électronique, le législateur sud-africain liste de manière non-limitative les éléments qui peuvent être considérés comme des « personal informations ». Il cite notamment les empreintes digitales, le groupe sanguin.
Le modèle sud-africain présente la particularité d'être l'un des plus anciens à utiliser la biométrie sous la forme d'empreintes digitales, pour l'identification des individus. Durant la longue période de l'apartheid, un registre national de la population[305] a été constitué. Il s'agissait d'une base de données contenant des informations d'identification officielles, comme la date de naissance, le décès, le mariage, la « race » des individus ainsi qu'un gabarit de leurs empreintes digitales. Les services de police sud-africains ont rénové leur base de données d'empreintes digitales à l'aide d'un système informatique qui permet leur numérisation. Ce répertoire peut être consulté par les citoyens depuis le Promotion to Access Information Act de janvier 2000.[306]
La biométrie permit également de réguler les déplacements des travailleurs employés dans les mines d'or. Cette méthode fut ensuite étendue à l'industrie. Forte de son

---

[299] Section 14
[300] http://www.law.wits.ac.za/salc/salc.html/
[301] « techniques of personal identification that are based on physical characteristics. Biometric techniques include fingerprint, retinal scanning and voice recognition »
[302] « Any information relating to an identified or identifiable natural (or juristic) person. An identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one more factors specific to his physical,physiological, mental, economic, cultural or social identity »
[303] Personal Information
[304] ECT Act : loi de régulation du commerce électronique du 30 août 2002
[305] National population register
[306] http://www.privacyinternational.org/countries/ south africa/access info bill.pdf

expérience en matière de reconnaissance digitale, l'Afrique du Sud offre un exemple intéressant de l'utilisation de la biométrie pour l'octroi d'avantages. En effet, comme l'indique Keith Breckenridge, la première application à grande échelle de la biométrie digitale a concerné la délivrance des pensions dans l'état du KwaZulu en 1990[307]. L'état du KwaZulu a rencontré de nombreuses difficultés dans l'allocation des pensions au sein des zones rurales, et, pour pallier ces difficultés, a mis en place un système biométrique. Les bénéficiaires des pensions ont procédé à l'enregistrement de leurs empreintes digitales qui étaient stockées sur une carte magnétique et dans une base de données. La pension était alors délivrée après reconnaissance de l'empreinte qui était lue par un scanner relié à un ordinateur.

Diverses provinces ont adopté cette solution

Les cartes ont par la suite évolué ; plusieurs fonctions y furent introduites. La carte approvisionnée par le versement de la pension fut utilisée comme carte de retrait ; néanmoins, elle ne servit de moyen d'identification que de manière secondaire ; sa finalité principale demeurait la suivante : permettre aux habitants des provinces reculées de recevoir les divers émoluments auxquels ils peuvent prétendre. En 1999, la Smartcard a été utilisée comme moyen de paiement dans les taxis et les moyens de transport qui desservaient les provinces reculées. L'utilisation de la carte en tant que moyen de paiement a été étendue au règlement des factures des services tels que l'eau, l'électricité et l'alimentation. La Smartcard a servi également de support à l'octroi de micro-crédit.

La société gestionnaire de ce système a permis à certains fournisseurs de services et aux assurances d'effectuer des prélèvements automatiques sur le compte du titulaire de la carte. Aplitec a été victime de son succès, dont l'efficacité et l'intérêt ont été altérés par les diverses possibilités d'octroi de crédit.

Le registre national de la population (Nation population Register) est une survivance de l'apartheid géré par le ministère des affaires intérieures (Department of Home Affairs). Cette base de données contenait des informations d'identification officielle sur la date de naissance, le décès, le mariage, la race des individus et un gabarit de leurs empreintes digitales. La population s'est considérablement accrue, les fichiers papiers se sont détériorés, ont été difficilement conservés et parfois consultés. Devant cette multiplicité d'aléas, il a été envisagé en 1993 de remplacer le registre par un système informatisé d'identification biométrique. Il s'agit du Hanis pour Home Affairs National Identification System. Il est basé sur la reconnaissance des citoyens à l'aide des empreintes digitales (Automated Fingerprint Identification System)[308]. Un projet plus performant avait été élaboré en 1996 mais il n'a pas encore vu le jour. Il consistait à installer deux systèmes de biométrie digitale, l'une réservée à l'administration civile, l'autre à la justice criminelle.

Le programme conférerait un unique identifiant à chaque individu utilisable dans le secteur privé comme dans le secteur public. Il était prévu à long terme que ce mode d'identification permette l'octroi de pensions et trouve un usage dans le secteur de la santé et dans le domaine de l'aide sociale.

Quant à Hanis, il a été remplacé par une « smart card » fonctionnant sur trois niveaux d'identification : une vérification visuelle, une vérification en ligne par la consultation de la base de données et une vérification hors ligne. Tous ces niveaux de vérifications devraient permettre d'assurer la sécurité des transactions électroniques en ligne. La

[307] http://wiserweb.Wits.ac.ZA/PDF%20Files/state%20-%20breckenridge.PDF, article de Keith Breckenridge « Biometric Government in the New South Africa »

[308] AFIS cf : le site du ministère de l'intérieur sud-africain http://home-affairs.pwv.gov.za

smart card servirait d'identifiant unique. Cela induit de nombreux problèmes en matière de libertés individuelles. L'instauration d'un tel mode d'identification serait impossible en Europe.
Le contenu de la carte biométrique est aussi fiable que celui de la base de données et aussi fiable que le gabarit collecté lors de la numérisation de l'empreinte digitale. Les possibilités d'erreurs et de fraudes dans la base de données préexistante sont réelles. Certaines personnes physiques peuvent avoir la même empreinte digitale. Enfin des problèmes de sécurité se posent : ils concernent l'accès à la base de données et la puce de la carte proprement dite. Il convient de prévoir un redéploiement de Hanis et un système de cryptographie pour les données.[309]
L'apartheid a donc induit le développement d'une culture biométrique ; à présent que l'apartheid appartient à un passé révolu, la culture biométrique demeure. Les empreintes digitales ne sont pas seulement l'apanage des autorités policières ; elles constituent un moyen d'identification pour divers acteurs. Une étude sociologique nous renseignerait utilement sur les relations qu'entretiennent les Sud-Africains avec cette culture biométrique.

BIOMETRIE ET SIGNATURE ELECTRONIQUE

La problématique de la valeur probatoire des documents électroniques et de la signature électronique est au cœur des préoccupations des juristes à la fin du vingtième siècle et au début du vingt-et-unième siècle.
Avec le développement exponentiel de l'Internet et du commerce électronique, les transactions sont sécurisées par la cryptologie. Si les développements sur la sécurisation par la cryptologie sont pertinentes et suffisamment nombreuses, les sources documentaires sur les rapports entre biométrie et signature électronique sont encore insuffisantes.
La CNUDCI[310] est à l'origine de références incontournées, des « lois-types » sur le commerce électronique.

L'UNION EUROPEENNE

La directive de l'Union européenne du 13 décembre 1999 précise le régime de la signature électronique et de la signature électronique avancée, garantie par des prestataires de services de certification et des certificats, basés sur la cryptographie symétrique et sur la cryptographie asymétrique. Elle met en place le régime de la certification.

La loi française du 13 mars 2000 révise le Code Civil. Les documents électroniques, sous conditions d'identification et d'intégrité, deviennent des preuves littérales. La signature électronique exprime le consentement des contractants, tant dans les contrats solennels que dans les contrats sous seing privé. Le droit français[311]introduit la signature électronique sécurisée, transposition de la signature électronique avancée. La cryptologie permet l'identification et l'authentification.

---

[309] http://wiserweb.wits.ac.za/PDF%20Files/state%20-%20breckenridge.PDF article de Keith Breckenridge « Biometric Government in the New South Africa »
[310] Commission des Nations Unies pour le droit commercial international
[311] Décret du 30 mars 2001, arrêté du 31 mai 2002

I) L'adoption de la loi du 13 mars 2001 a été précédée d'une consultation publique. A)L'un des principaux thèmes discutés est l'élimination de la signature dynamique, au profit de la signature numérique. L'élément qui traduit la priorité accordée par la loi à la signature numérique est l'intégrité. Avant l'échange électronique, un condensé du texte a été fait. Le destinataire qui vérifie la signature électronique contrôle si le condensé est identique. La signature numérique présente un lien puissant avec le texte signé. L'intégrité concerne l'état du document arrivé à destination après transmission électronique.

B) La critique doctrinale de Thierry Piette-Coudol : en amont du projet de loi, Thierry Piette-Coudol émet des critiques sévères, qui ne seront d'ailleurs pas prises en compte.

Le terme « électronique » est trop étroit. Il induit un danger d'obsolescence rapide.

La signature électronique s'appuyant sur la cryptographie asymétrique et les tiers certificateurs correspond plus à un sceau d'authenticité électronique qu'à une signature au sens juridique du terme.

La décision d'accorder une validité juridique à la signature électronique peut perturber le marché des prestataires de services de certification qui n'ont pas toujours développé de fonction ou d'objectif juridique.

La loi ne vise que les signatures numériques[312] et élimine la signature dynamique[313]qui utilise l'accélération dans les mouvements de la main.

La signature numérique basée sur la cryptographie est définitivement adoptée.

II) Biométrie et signature électronique : depuis l'an 2000, il est apparu que la biométrie pouvait se mettre au service de la signature.

A) Une politique d'offres a été mise en place par les industriels.

« Sécuriser une transaction en la cryptant ou en authentifiant les interlocuteurs avec un code ou un mot de passe, ce n'est pas suffisant »[314]tel est l'avis des industriels. Ces derniers travaillent sur l'authentification de la signature électronique.

Ainsi, l'entreprise Zalix a-t-elle développé dès l'an 2000 une solution d'authentification de la signature électronique[315]. La solution repose sur l'utilisation d'une tablette graphique Wacom ou d'un Palm Pilot et du logiciel Penflow[316]. Plus de cent paramètres sont pris en compte par le logiciel : pression du stylo, la rapidité d'exécution, l'inclinaison du stylo, etc….

Les utilisateurs auront au préalable enregistré le profil de leur signature[317]. La signature, cryptée, est stockée dans une base de données. Lors de la saisie dynamique de la signature sur la tablette, le logiciel envoie l'information au serveur Web hébergé chez Zalix pour authentification. Le serveur extrait le profil de la base, le décrypte puis le compare à la signature à valider avant de renvoyer un avis, favorable ou défavorable. Une signature à l'identique de celle stockée dans la base sera rejetée[318]

Zalix propose aussi une authentification par l'empreinte digitale.

« Le dispositif répond aux exigences de l'article 1316-1 du Code civil, portant adaptation du droit de la preuve aux technologies de l'information, et relative à la signature électronique » déclarait Laurent Saada. Les conditions requises sont en effet

---

[312] basées sur la cryptographie asymétrique

[313] basée sur la biométrie comportementale

[314] Opinion de Laurent Saada, alors PDG et co-fondateur de la start-up Zalix, spécialisée dans la biométrie, citée dans JDNet solutions, 6 juin 2000

[315] Identi'sign

[316] Logiciel de reconnaissance d'écriture édité par la société israelienne Wondernet

[317] Trois signatures sont exigées pour l'enregistrement

[318] Zalix constate que personne ne signe deux fois de la même façon

réunies : identification des interlocuteurs, intégrité du document[319], non-répudiation : l'émetteur et le destinataire ne peuvent nier l'envoi et la réception du document[320].
Ce système a essentiellement pour cible le secteur bancaire[321]
De son côté, Actronix propose un système de reconnaissance biométrique conjointe à une signature électronique. Une mesure biométrique est liée à l'identité du signataire. L'écrit électronique est personnalisé par l'apport de la mesure biométrique.

LES USA

Les USA ont adopté le 30 juin 2000 une loi portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique par l'Electronic Signatures in Global and National Commerce Act ou « E-sign » du 30 juin 2000, entré en vigueur en octobre 2000. Cette loi permet comme en France d'inclure dans la définition de la signature[322] la signature électronique. Selon les commentateurs, la signature électronique peut consister en un simple nom ou en un procédé plus complexe et plus sûr telle qu'une technique biométrique. Cette interprétation peut aisément être retenue pour le E-Sign Act.[323]
Dans le monde de l'entreprise, Segugen Corporation s'associe à Digital Signature Trust en l'an 2000.[324]Digital Signature Trust est l'un des premiers organismes de certification licenciés aux USA. Ces industriels ont insisté sur la compatibilité entre la biométrie et les certificats. C'est pourquoi Segugen est en mesure de proposer une solution efficace de cybercommerce, qui renforce la protection cryptée. Segugen Corporation, fournisseur de solutions biométriques[325], est spécialisé dans la technique des empreintes digitales. L'association entre Segugen Corporation et Digital Signature Trust favorise la sécurité dans le domaine des transactions électroniques.
Il ne semble pas qu'il existe d'incompatibilité entre la signature électronique, la cryptographie asymétrique et l'identification biométrique.
Par contre, il peut exister des dérives en matière de libertés individuelles, surtout si l'identification biométrique est réalisée grâce aux empreintes digitales, généralement circonscrites dans le secteur policier, voire dans le contrôle des flux migratoires. Si les empreintes digitales sont utilisées comme élément d'identification dans le cadre de la signature électronique, les empreintes seront stockées par des personnes privées.
Entre la quasi certitude d'identification et le danger pour la vie privée, il convient de parvenir à un équilibre, qui implique le recours à un procédé biométrique d'authentification qui ne soit pas l'empreinte digitale.[326]

INFRASTRUCTURE PROTEGEE ET PAYS-BAS

[319] Aucune altération n'est subie en cours de transmission
[320] La signature est numérisée ; le destinataire s'identifie pour lire le document
[321] Selon Christophe Guillemin, « Protection des systèmes : le bel avenir de la biométrie », Zdnet France, 14 juin 2000
[322] Définie comme un écrit ou un autre signe permettant d'identifier son auteur, apposé sur un document en vue de son authentification ou pour qu'il produise des effets juridiques
[323] Cf : Laurence Bimbaum-Sarcy et Florence Darques « Electronic signature Comparison between French&US law » in International Business Law Journal, avril 2001, peut être consulté sur http://www.signelec.com
[324] L'an 2000 correspond à l'adoption de lois sur la signature électronique (USA, France)
[325] Qui a son siège dans la Silicon Valley
[326] Afin d'éviter le détournement de fichiers.

L'organisation des tribunaux du ministère hollandais de la Justice a opté pour une solution combinant le logiciel Utimaco et MaXware Benelux pour instituer son infrastructure protégée d'après la fonctionnalité de l'ICP et des services de répertoires.

La biométrie est utilisée dans les cartes à puce qui servent lorsque l'empreinte digitale du détenteur a été vérifiée. Cette solution permet d'authentifier les utilisateurs, les signatures numériques et de protéger les messages électroniques, les documents personnels.

CONCLUSION

L'enjeu juridique principal réside dans l'équilibre entre la sécurité et la liberté. A court terme, voire à moyen terme, la sécurité semble l'emporter sur toute autre considération. Ce sont les lois entrées en vigueur dans les pays occidentaux qui ont permis le décollage de l'industrie de la biométrie. Cette dernière n'est pas une panacée. Elle fait partie des moyens utilisés dans le cadre de la finalité sécuritaire.

Au niveau international, la normalisation progresse lentement, mais sûrement. L'OACI souhaite utiliser les techniques biométriques.

Tous les continents sont intéressés par les technologies biométriques. Certes, les industries et les recherches en matière de biométrie se concentrent surtout en Amérique du Nord, en Océanie, en Europe. Pour l'instant, les transferts de technologie en la matière sont rarissimes.

Les usages sont surtout collectifs et ont essentiellement pour but de maîtriser les flux migratoires. Aux USA, au sein de l'Union européenne, en Australie, les autorités se préoccupent de contrôler, via la biométrie, les demandes d'asile et les tentatives d'immigrations clandestines ou irrégulières. La biométrie, qui est essentiellement, au début du vingt-et-unième siècle, utilisée par les pays du « Nord » semble prête à rejeter le trop plein de population du « Sud ». Même si les entreprises de biométrie sont essentiellement occidentales, arrimées à des pays développés, les techniques biométriques intéressent tous les Etats en veine de sécurité. En Afrique, les pays du Maghreb, l'Ouganda utilisent l'outil biométrique. L'Ouganda[327], notamment, a recours à la reconnaissance faciale. La Commission électorale ougandaise a décidé, au début du vingt-et-unième siècle, de ficher ses onze millions d'électeurs. Elle a accordé le contrat à la société Viisage du Massachussets. Le cahier des charges prévoyait la prise de photos des onze millions d'électeurs en soixante jours et la mise en place d'une base de données qui détecte les imposteurs en moins de six secondes. Le système Facefinder, initialisé par Viisage, analyse l'agencement de 128 caractéristiques faciales pour procéder à l'identification. Le système n'est pas complètement fiable. Utilisé à Tampa,[328]à l'occasion du Super Bowl, il a généré un nombre relativement important d'erreurs. Quoi qu'il en soit, le système est entré en vigueur en Ouganda.

L'identification biométrique, via les empreintes digitales a également été utilisée pour les élections législatives et communales en Mauritanie : dans ce pays, l'objectif est de renforcer la démocratie en empêchant les fraudes qui avaient tendance à se multiplier auparavant. Il semble que l'intervention de la biométrie dans les opérations électorales en Mauritanie a permis une certaine régulation. Un projet d'expérimentation concerne le Mali.

Sur un autre continent, en Amérique du Nord, le Mexique a installé 2000 Morphotouch'[329],stations d'enregistrements biométriques, à l'Institut Fédéral électoral du

[327] Indice de développement humain : 158 ème rang sur 174 pays ; taux de mortalité infantile : 84/ 1000 naissances

[328] En Floride

[329] Sagem

Mexique pour l'authentification des cartes d'électeurs. Dans ce cas, il s'agit, non pas d'identifier, mais d'authentifier, ce qui est beaucoup complexe. L'opération semble avoir été menée à bien.
Les techniques biométriques sont aussi utilisées dans le domaine de l'état civil pour certains Etats en voie de développement.
En Côte d'Ivoire, l'état civil ivoirien a été modernisé grâce à un système de numérisation des registres et à un système de cartes d'identité et de cartes de résidents, basé sur une délivrance sécurisée par un double contrôle des données d'état civil et des données biométriques du demandeur[330].
Au Nigéria, il s'est agi, non pas de moderniser, mais de constituer l'état civil. A été initialisé un système de production de cartes d'identité. Les autorités ont procédé à un recensement, à une élaboration de la base de l'état civil, à la production des titres d'identité, à l'authentification par les empreintes digitales. L'implémentation de techniques biométriques dans les pays en voie de développement, notamment en Afrique, prend en compte le référentiel culturel, tout en contribuant à son évolution. L'attachement à une ethnie, à une tribu cède le pas à un processus d'individualisation, qui participe à la modernisation[331]des différents Etats.
Ainsi, malgré les apparences, les techniques biométriques ne sont pas l'apanage des « pays du Nord ». Elles participent, au même titre que l'Internet, à l'apparition des nouvelles technologies dans des pays divers, très, moyennement ou peu développés.
L'équilibre à instaurer entre sécurité et liberté est difficile à maintenir.
Les données biométriques apparaissent partout comme des données personnelles mais le statut alloué en matière de données personnelles varie selon les pays et les régions. En Europe, au Canada, la protection des données personnelles est régie par la loi. En conséquence, les détournements de finalité sont interdits en matière de techniques biométriques. Dans la mesure du possible, il est tenu compte de la culture et du consentement des personnes concernées. Aux USA, la sauvegarde des libertés individuelles n'est pas actuellement une priorité et les techniques biométriques sont fréquemment utilisées sans que l'homme de loi ne se pose de questions particulières.
Au niveau international, malgré la résolution de 1990 sur la protection des données personnelles[332], l'ONU ne se préoccupe pas toujours des données . Ainsi, le HCR n'a-t-il pas pris de précautions particulières à l'occasion du retour de familles afghanes après un long séjour au Pakistan.[333] Depuis le début de l'année 2003, le HCR[334] a pris en charge le rapatriement de 380000 personnes. 130000 personnes se seraient pliées à la procédure d'identification par l'iris instaurée dans trois centres sis dans la région de Peshawar. Le système a été testé à partir d'octobre 2002 puis généralisé en 2003. Après l'examen d'identification, les réfugiés perçoivent une aide au transport, des bons alimentaires, des objets de première nécessité. Le HCR justifie le recours à l'identification biométrique par la nécessité de lutter contre la fraude à l'aide alimentaire. Il y aurait proportionnalité entre la finalité poursuivie et le recours à la technique de l'iris. L'agence onusienne déclare avoir repéré environ 600 cas de repasse. Au delà de ce chiffre assez faible, le HCR estime avoir économisé des millions de dollars en décourageant les fraudeurs potentiels[335].A la mi-juillet,le

[330] Empreintes digitales
[331] Certains pensent : à l'occidentalisation
[332] Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, adoptés le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 199à
[333] Plus de 2,3 millions d'Afghans se seraient réfugiés au Pakistan et en Iran
[334] Haut-commissariat des Nations-unies pour les réfugiés
[335] cf : déclaration de Kris Janowski, porte-parole de l'agence, lors d'une réunion de presse en date du 8 août 2003

Haut-Commissariat a renforcé la procédure : alors que le contrôle était obligatoire jusqu'alors pour les mineurs de douze ans, il est devenu obligatoire pour les enfants de six ans et plus ; des adultes utiliseraient les enfants et les jeunes à des fins frauduleuses. De plus, le HCR déclare que sa base de données n'associe les images des iris à aucun nom patronymique, ni aucune autre information personnelle. Il serait donc en règle avec la résolution de 1990. Selon l'organisation non-gouvernementale Statewattch.org, un contrôle aussi intrusif ne devrait pas s'appliquer à de jeunes enfants. Cela constituerait une viol[336]ation de la Convention des Nations Unies relative aux droits de l'enfant et notamment de son article 16 « Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation ». Statewatch revient aussi sur les données personnelles en dénonçant les risques de fichage à grande échelle. La lutte contre la fraude alimentaire semble dérisoire. La fraude est générée par la pauvreté[337]. Le HCR réplique sur le terrain des données personnelles en arguant qu'il ne partage pas ses données avec les gouvernements, sauf cas exceptionnels. Le débat reste ouvert.

Quant à l'OACI, qui dépend aussi des Nations Unies, elle impose en mars 2003 la reconnaissance faciale pour les documents de voyage. Elle est favorable à l'usage de la puce, protectrice en matière de donnés personnelles. Le bilan est donc mitigé. Les organismes spécialisés prennent en considération les normes relatives aux données personnelles mais souhaitent utiliser les techniques biométriques à des fins sécuritaires.

L'objectif sécuritaire apparaît plus que jamais dans la multiplication des passeports et des cartes nationales d'identité biométriques.

La position intransigeante des USA, qui exigent en 2003 des passeports avec lecture optique et, à partir du 1 octobre 2004, des passeports biométriques, amène de nombreux pays, dont les citoyens se rendent fréquemment aux USA[338] à imposer progressivement les applications biométriques.

Les Etats les plus attachés aux libertés individuelles[339]s'interrogent sur l'introduction de cartes d'identité nationale quand ni la loi ni les usages ne les avaient imposées précédemment. Le débat met en exergue les points de vue développés par le ministre de l'intérieur d'une part, les opinions et les assertions des associations de défense des droits de l'homme, d'autre part, surtout quand la carte d'identité est biométrique.

En Chine, il a été décidé d'introduire une carte d'identité. Cela correspond à un souci d'aménagement du territoire. En effet, le développement accéléré du capitalisme chinois a induit des contrastes dommageables pour la démographie et pour l'écosystème. Un certain nombre de ville regroupent non seulement les agents les plus actifs du libéralisme économique, mais aussi des ruraux en quête d'un emploi et de biens de consommation courants. La désertification de certaines campagnes préoccupe les autorités locales et nationales. Il convient, dans cette optique, urgent de canaliser ces mouvements de population, d'identifier les personnes qui quittent le monde rural pour la ville. En effet, aucun retour n'est envisageable. Or, le paysan chinois a été l'unité de base de la révolution chinoise, des stratégies décidées par Mao-tsé-toung et ses successeurs convertis à l'économie de marché. En 2003, le gouvernement chinois avait opté pour une carte d'identité biométrique, et pour l'utilisation de l'ADN. Très vite, les autorité chinoises ont réalisé que le taux de faux rejets et de fausses acceptations serait trop élevé et que les dérives risquaient d'être trop nombreuses.

---

[336] Adoptée en 1989

[337] « Ce que l'on voit, au delà de cette affaire, c'est le discours condescendant du HCR à propos de gens qui sont si désespérés qu'ils tentent de récupérer quelques dollars et un peu plus de nourriture. Cela devrait pousser le HCR à s'interroger de manière urgente sur les conditions de vie en Afghanistan plutôt qu'à les considérer comme des criminels » écrit Tony Bunyan, l'un des responsables de Statewatch,2003

[338] C'est le cas de la plupart des Etats de l'Amérique latine et de l'Union européenne

[339] Cf : Canada

Le réalisme a triomphé assez aisément. Cependant, la piste biométrique est désormais suivie en Chine et donnera vraisemblablement lieu à de nouvelles expériences, qui seront sans doute une source de profits appréciables sur un marché important.
Ainsi, la biométrie est-elle présente sur tous les continents. Les usages sont davantage collectifs que domestiques. Or, ce sont précisément les usages collectifs qui posent le plus de problèmes sur le plan juridique. L'équilibre entre l'objectif de sécurité et le respect des libertés individuelles semble difficile à atteindre. Ce sont les finalités sécuritaires qui ont permis le développement des applications biométriques. Ce sont les profits dégagés dans le cadre de la politique sécuritaire qui ont financé des recherches nouvelles dans la biométrie qui trouveront des applications sécuritaires. Le contexte géo-politique n'est pas non plus favorable au libéralisme juridique. Les USA constituent l'unique puissance prééminente à l'échelle planétaire et ce statut n'est pas près d'être remis en cause. Or, ce sont les USA qui ont initié le courant liberticide[340] à l'origine de la croissance des utilisations biométriques. Les puissances régionales émergentes, tels la Chine et le Brésil, ne sont guère attachés aux droits de l'homme. La configuration politique des dix prochaines années va dans le même sens. Pourtant, les applications biométriques peuvent être utilisées à d'autres fins que la sécurité. La voiture biométrique, la maison biométrique permettront des usages intéressants. Le droit joue un rôle d'arbitre dans les investissements actuels. Il reste donc à espérer que l'équilibre sécurité/liberté connaîtra un infléchissement plus favorable que nous l'escomptons.

BIBLIOGRAPHIE

CNIL, 21ème rapport d'activité, p 101 à 120, 2000
Rapport Cabal (Christian) sur les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en oeuvre, Assemblée Nationale, juin 2003
Intelligence on line

WEBOGRAPHIE

www.transfert.net
www.zdnet.com
www.zdnet.fr
www.privacyinternational.org
www.telecom.gouv.fr
www.vnunet.fr
www.interpol.int
www.solutions.journaldunet.com
www.biometrie.online.fr
www.juris-net.net/
www.be.adit.fr/japan/
www.goethe.de/mmo/priv/
www.cic-forum.ca/

[340] Avec le « Patriot Act » notamment

INDEX