CHAMBRE DES SALARIES
LUXEMBOURG

27 mars 2009

AVIS I/9/2009

relatif au projet de loi relatif à l'identification des personnes physiques, au registre national des personnes physiques et à la carte d'identité

..... AVIS .....

18 rue Auguste Lumière L-1950 Luxembourg
B.P. 1263 L-1012 Luxembourg
T. +352 48 86 16-1 F. +352 48 06 14
csl@csl.lu www.csl.lu

Par lettre en date du 28 octobre 2008, Monsieur Claude Wiseler, Ministre de la Fonction publique et de la Réforme administrative a fait parvenir à notre chambre professionnelle le projet de loi relatif à l'identification des personnes physiques, au registre national des personnes physiques et à la carte d'identité.

1. Objectifs du projet de loi

Le présent projet de loi a pour objet de réformer le système d'identification des personnes physiques en créant, d'une part, un registre national des personnes physiques (RNPP) qui remplace l'actuel répertoire général des personnes créé par la loi du 30 mars 1979 et en introduisant, d'autre part, une carte d'identité électronique à l'aide de données biométriques (reconnaissance faciale).

Le système actuel du répertoire général des personnes physiques et morales ne permet plus de garantir que toutes les données répertoriées soient exactes et ne permet donc pas de les considérer comme authentiques. Le fait que beaucoup d'administrations ont créé leurs propres banques de données sur base de critères qui n'étaient pas toujours identiques et le fait que ces bases de données qui ont alimenté le répertoire général des personnes, n'ont pas toujours été mises à jour simultanément, ont rendu l'identification des personnes disparate et peu fiable.

Il en va de même pour l'identification personnelle des citoyens qui résulte en somme de la fiabilité des données figurant dans le répertoire général des personnes. Avec l'introduction du nouveau répertoire national des personnes physiques, le gouvernement a profité d'introduire une carte d'identité électronique qui devra être à l'abri de falsifications. Afin de réduire les abus, la carte d'identité électronique sera dotée d'une photographie numérisée du titulaire et la délivrance sera confiée à quatre centres administratifs de l'Etat situés à Luxembourg-Ville, Esch/Alzette, Diekirch et Grevenmacher, disposant d'équipements appartenant à l'Etat et situés dans des endroits sécurisés sur le territoire luxembourgeois.

Le présent projet de loi résume ses objectifs comme suit : d'une part, simplifier les charges administratives des citoyens en améliorant la collaboration entre les administrations et, d'autre part, renforcer la protection des données à caractère personnel.

La Chambre des salariés se doit de formuler un certain nombre d'objections.

2. Le nouvel système d'identification ne risque-t-il pas d'entraver davantage les libertés individuelles du citoyen ?

Si notre chambre, *à première vue,* peut témoigner de la compréhension pour cette réforme dans la mesure où celle-ci envisage de rendre plus fiables et sûres les données d'identification des personnes physiques, elle reste toutefois vigilante et sceptique en ce qui concerne l'usage et le contrôle de telles données qui tombent sous le champ d'application de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Elle craint que la présente réforme du système d'identification des personnes ne se situe pas seulement dans le contexte des motifs évoqués dans l'exposé des motifs du présent projet de loi, mais également dans un contexte plus vaste, à savoir celui de la lutte contre le terrorisme et d'une emprise croissante de l'Etat sur la sphère privée du citoyen.

Voilà pourquoi elle se doit de formuler un certain nombre d'objections qui concernent, avant tout, l'identification biométrique du citoyen par le biais de la carte d'identité électronique.

2.1. Les principes de finalité et de proportionnalité de l'identification biométrique sont-il garantis ?

La biométrie peut être définie comme recouvrant l'ensemble des procédés tendant à identifier un individu à partir de la « mesure » de l'une ou de plusieurs de ses caractéristiques physiques, physiologiques ou comportementales.

La biométrie peut *a priori* présenter un certain nombre d'avantages : sécurité accrue des données, protection et lutte contre la fraude ou le vol d'identité, non transmissibilité des données, identification positive, plus de confort par une diminution des charges administratives tant pour les administrations que pour les administrés etc. Par ailleurs, elle a un potentiel substantiel comme technologie de protection de données ("Privacy enhancing technology") en sécurisant l'accès à celles-ci.

Il faut cependant rester prudent quant aux utilisations qui peuvent en être faites, car au-delà de l'aspect technique, l'information biométrique est surtout une caractéristique propre à tout être vivant, un élément de la personne humaine, et de ce fait considérée en règle générale comme une donnée à caractère personnel. En conséquence, le recours à la biométrie peut présenter des risques quant au respect des droits et libertés fondamentales, y compris la protection de la vie privée et des données.

Il incombe de trouver un équilibre sain entre les intérêts de l'Etat et ceux du citoyen.

Afin de respecter les libertés individuelles du citoyen, notre chambre exige que l'utilisation des données à caractère personnel – et à plus forte raison les données biométriques - respecte le principe de la finalité et de la proportionnalité.

Le principe de finalité repose sur le postulat que la menace pour la vie privée que constituent les traitements de données à caractère personnel et, à plus forte raison, les traitements de données biométriques, réside davantage dans la finalité qu'ils poursuivent que dans la nature des données traitées. En d'autres mots, il importe de savoir plutôt « pourquoi » on recourt au traitement de données à caractère personnel que « en quoi » consiste le traitement.

Le principe de proportionnalité précise que les données doivent être nécessaires, et non seulement utiles, pour qu'un traitement puisse être accompli et qu'on renonce à traiter ou utiliser des données biométriques si l'identification ou l'authentification des personnes dans le cadre recherché peut être réalisé avec la même efficacité et sécurité sans de telles données et avec des moyens moins intrusifs.

Pour la Chambre des salariés, soucieuse de la protection des libertés individuelles du citoyen, les principes de la finalité et de la proportionnalité risquent d'être violés dans un certain nombre de cas de figure.

A titre d'illustration, notre chambre se permet de soulever les questions suivantes :

Qui garantit que lors d'un contrôle d'identité par la police, les données biométriques d'un individu ne soient pas détournées à des fins étrangères en comparant celles-ci au contenu d'une autre base de données faisant l'objet d'une autre finalité (par exemple la comparaison à une liste de terroristes recherchés) ?

Qui garantit que dorénavant les technologies de la biométrie ne soient pas utilisées pour poursuivre et détecter toutes infractions quelconques, de quelque gravité qu'elles soient, voire même pour contrôler toute personne en amont d'une infraction ?

En raison des questions soulevées ci-avant, notre chambre se demande si l'argument tous azimuts de la sécurité de l'Etat et de la lutte contre le terrorisme ne sert pas de prétexte pour justifier l'introduction de nouveaux systèmes d'identification des personnes par des technologies de plus en plus sophistiquées réduisant progressivement à néant les libertés fondamentales du citoyen.

2.2. Le contrôle du traitement des données biométriques

La loi modifiée du 2 août 2002 prévoit que les traitements de données biométriques nécessaires à l'identification des personnes concernées doivent être autorisés préalablement par la Commission nationale de la protection des données (CNPD).

L'article 25 du présent projet de loi dispose toutefois que *« tout contrôle automatisé de cartes d'identité par des procédés de lecture optique ou autres doit faire l'objet d'une autorisation du ministre sur avis conforme de la commission du registre national »* .

Notre chambre se doit de constater que le législateur, au lieu de se référer à la Commission nationale de la protection des données en ce qui concerne le recours à des procédés de lecture optique de cartes d'identité, confie cette tâche au ministre ayant le Centre informatique de l'Etat dans ses attributions, sur avis conforme de la commission du registre national dont la composition et le fonctionnement peuvent être déterminés par règlement grand-ducal.

Est-il justifié d'attribuer le contrôle automatisé de cartes d'identité au ministère qui est chargé de toutes les opérations relatives à la détermination, à l'attribution et à la conservation des données à caractère personnel alors que cette tâche relève, en vertu de l'article 32 de la loi modifiée du 2 août 2002 citée ci-avant, de la compétence de la CNPD?

Notre chambre est d'avis qu'en tout état de cause, il incombe à la CNPD de vérifier le bien-fondé des contrôles automatisés de cartes d'identité, à défaut de quoi le ministère risque d'être à la fois juge et partie.

De façon plus générale, notre chambre exprime ses plus grands doutes en ce qui concerne l'efficacité du contrôle de traitements de données à caractère personnel – parmi lesquelles figurent les données biométriques - dans la mesure où le contrôle est de moins en moins exercé par la CNPD et dans la mesure où bon nombre de traitements de données à caractère personnel échappent au contrôle de la CNPD, parce que celle-ci n'a tout simplement pas été informée par le responsable du traitement.

2.3. Le droit à l'information de la personne concernée : lacunaire et peu efficace !

En ce qui concerne le RNPP, l'article 16 du projet de loi prévoit la faculté pour le citoyen de demander la communication de ses données. Toutefois ce droit ne protège en rien les libertés individuelles du citoyen alors qu'il est dans l'impossibilité de vérifier la traçabilité et le bien-fondé des traitements de ces données communiquées à des tiers. L'article 16 permet uniquement à l'individu de demander la liste des autorités qui ont, au cours des six mois précédant sa demande consulté ses données sur le RNPP, mais non pas les raisons pour lesquelles ces données ont été consultées.

Abstraction faite de l'efficacité d'un tel droit, il y a lieu de signaler qu'un tel droit d'information n'existe pas pour les données biométriques alors que celles-ci ne figurent pas sur le RNPP. En effet, l'article 27, paragraphe 3 dispose que les données biométriques ne sont conservées que pendant une durée de 2 mois après la délivrance de la carte d'identité, mais ne prévoit ni l'endroit où ces données sont conservées ni le droit à l'information de la personne concernée.

Notre chambre est d'avis que les dispositions précitées sont contraires à l'article 26 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel pour les raisons suivantes :

- En ce qui concerne les données biométriques qui sont collectées directement auprès de la personne concernée, le paragraphe 1 de l'article 26 de la loi précitée dispose que

« le responsable du traitement doit fournir à la personne concernée, au plus tard lors de la collecte

et quels que soient les moyens et supports employés, les informations suivantes, sauf si la personne concernée en a déjà été informée de :

(a) l'identité du responsable du traitement et, le cas échéant, de son représentant ;

(b) la ou les finalités déterminées du traitement auquel les données sont destinées ;

(c) toute autre information supplémentaire telle que :

- *les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées ;*

- *le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse ;*

- *l'existence d'un droit d'accès aux données le concernant et de rectification de ces données ;*

dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données. »

Voilà pourquoi notre chambre propose de compléter l'article 27, paragraphe 3 du projet de loi par la phrase suivante : « Le droit à l'information de la personne concernée au sujet de ses données biométriques est régi par l'article 26, paragraphe 1 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ».

- En ce qui concerne les données inscrites sur le RNPP (article 23 du projet de loi) lesquelles alimentent également le registre des cartes d'identité (article 27 du projet de loi), à l'exception des données biométriques, et qui proviennent non pas directement des individus, mais des différents autorités et organismes étatiques, le paragraphe 2 de l'article 26 de la loi modifiée du 2 août 2002 précitée est de la teneur suivante :

« Lorsque les données n'ont pas été collectées auprès de la personne concernée, le responsable du traitement doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée sauf si elle en a déjà été informée de :

(a) l'identité du responsable du traitement et, le cas échéant, de son représentant ;

(b) la ou les finalités déterminées du traitement auquel les données sont destinées ;

(c) toute information supplémentaire telle que :

- les catégories de données concernées ;

- les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées ;

- l'existence d'un droit d'accès aux données le concernant et de rectification de ces données ;

dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données. »

La Chambre des salariés est d'avis que les articles 13 à 22 du présent projet de loi sont contraires à l'article 26, paragraphe 2 de la loi modifiée du 2 août 2002 précitée et qu'il importe par conséquent de les y adapter .

2.4. La fiabilité des données biométriques

Notre chambre se doit de constater que l'exposé des motifs du projet de loi ne soulève aucunement les problèmes de fiabilité de la biométrie.

La biométrie présente un inconvénient majeur ; en effet aucune des mesures utilisées ne se révèle être totalement exacte car il s'agit bien là d'une des caractéristiques majeures de tout organisme vivant : on s'adapte à l'environnement, on vieillit, on subit des traumatismes plus ou moins importants, bref on évolue et les mesures changent.

Pour la reconnaissance faciale[1], il est facile d'imaginer les nombreuses approches possibles pour entreprendre l'analyse des caractéristiques d'un visage, ce qui donnera lieu à des performances disparates en fonction de leurs capacités à prendre en compte des situations diverses comme l'éclairage, l'arrière-plan, le sourire/rictus de la personne, l'angle/l'inclinaison de sa tête, la présence d'une moustache ou d'une barbe, le port de lunettes, le vieillissement etc.

Le cumul de toutes ces incertitudes et causes d'erreur a pour conséquence qu'en toute rigueur, un système de contrôle biométrique ne peut donner, lors d'une comparaison entre deux échantillons biométriques, qu'un résultat sous forme de probabilité de coïncidence.

Puisque le résultat d'une comparaison est toujours une estimation (un score), tous les systèmes biométriques donnent la possibilité de paramétrer le seuil d'acceptabilité :

- soit en exigeant du système un contrôle strict, en mettant par exemple le seuil à 99,8%, signifiant par-là que 2 échantillons ne seront considérés comme provenant d'un même individu que si le score de similitude est supérieur à 99,8% ;

- soit en étant plus tolérant, en autorisant par exemple que le système réponde positivement si le score de similitude n'est pas en dessous de 95%.

Avec la première option, la conséquence mécanique sera d'augmenter le nombre de « faux rejets », c.-à-d., par exemple lors d'un contrôle, d'augmenter le nombre de refus de personnes qui ne sont pourtant pas en fraude.

La seconde option aura pour conséquence d'augmenter le taux de « fausses acceptations », c.-à-d., d'accepter comme identiques des échantillons biométriques qui, en réalité, proviennent d'individus différents. La fraude sera plus facile.

L'appréciation doit donc se faire au cas par cas, l'incidence des applications sur la protection de la vie privée et des données à caractère personnel différant aussi selon la technologie biométrique utilisée. Il faut donc non seulement veiller à garder en juste équilibre notamment la finalité et la proportionnalité de l'application, mais également évaluer selon des critères pertinents les risques que présente la technique appliquée par rapport à la protection des données à caractère personnel. Alors qu'une telle appréciation contient un certain degré d'approximation du fait des variations possibles des éléments, les critères communément invoqués sont les suivants:

Fiabilité - taux d'erreurs (fausses acceptations et faux rejets) important ou faible ? La reconnaissance faciale ou vocale, la géométrie du doigt et la dynamique de la signature sont jugés être d'une fiabilité moindre par rapport à l'empreinte digitale ou la reconnaissance de l'iris.

Transparence de l'exploitation - application visible ou à l'insu des personnes concernées ? L'empreinte digitale, la géométrie de la main, la reconnaissance de la rétine ou encore la dynamique

[1] Ainsi la reconnaissance faciale ou vocale, la géométrie du doigt et la dynamique de la signature sont jugés être d'une fiabilité moindre par rapport à l'empreinte digitale ou la reconnaissance de l'iris.

de la signature sont des techniques considérées comme transparentes puisqu'elles ne peuvent être mises en œuvre sans que la personne concernée soit au courant.

Acceptabilité par les utilisateurs - l'acceptation de l'application dépend du caractère invasif ou non de la technique utilisée, la reconnaissance de la rétine étant ressentie comme plus dérangeante que la reconnaissance faciale.

Degré de stabilité de l'élément biométrique - constance d'une caractéristique au cours du développement et vieillissement normal d'une personne.

Coût - les technologies évoluent assez rapidement ; néanmoins la reconnaissance de l'iris ou de la rétine engendrent des coûts beaucoup plus importants que p.ex la reconnaissance vocale.

Facilité d'emploi - il s'agit ici d'apprécier le degré d'interaction possible avec le système, en partant des techniques les plus faciles d'utilisation et en terminant avec les plus difficiles: la reconnaissance faciale, la dynamique de la signature, la frappe sur le clavier, la reconnaissance vocale, l'empreinte digitale, la géométrie de la main, et enfin reconnaissance de la rétine.

Enfin, certaines biométries laissent des traces qui peuvent être utilisées et traitées à
l'insu de la personne concernée : c'est le cas de l'ADN, des empreintes digitales, et peut-être bientôt du visage (reconnaissance faciale) et de l'iris, si la vidéosurveillance se généralise et si la technologie de ces procédés progresse.

D'autres facteurs qui entrent également en considération ont trait à la fiabilité et la vulnérabilité des systèmes biométriques, aux problèmes d'interopérabilité, aux possibilités de traçage des individus ou à l'acceptabilité des techniques. La question de la conservation et du stockage des éléments biométriques mérite une attention toute particulière, la Commission nationale de l'informatique et des libertés (la CNIL étant l'équivalent français de la CNPD luxembourgeoise) notamment mettant en garde contre la constitution de bases de données, et préconisant des éléments biométriques "ne laissant pas de traces" (p.ex. contour de la main) si le stockage dans une base de données s'impose.

La biométrie n'est pas seulement un moyen d'identification susceptible de transgresser le principe de la finalité et de la proportionnalité, qui échappe le plus souvent au contrôle de la CNPD, mais elle constitue par ailleurs, selon les experts, un moyen peu fiable et, par là, dangereux pour la sauvegarde du droit à la vie privée du citoyen. Ce danger est encore accentué par le fait que la création de moult bases de données à caractère personnel, qui n'ont pas été notifiées à la CNPD ou qui n'ont pas reçu l'autorisation préalable par celle-ci, échappent à tout contrôle.

2.5. Le risque de création de bases de données à caractère personnel échappant à tout contrôle

Notre chambre craint qu'il n'existe une kyrielle de bases de données dont nul, à part les auteurs eux-mêmes, connaît leur existence.

Cette inquiétude est d'autant plus justifiée si l'on regarde les nombreux exemples récents d'espionnage que certaines entreprises en Allemagne ont mené à l'insu de leurs salariés (Siemens, Telecom, Deutsche Bahn, Lidl etc.) et qui n'ont percé à jour que par pure coïncidence. Un tel scénario n'est pas non plus exclu au Luxembourg.

La Chambre des salariés se doit de conclure que plus on harmonise (uniformise) les données à caractère personnel – parmi lesquelles les données d'identification des personnes – moins le justiciable sera sollicité lui-même par les responsables du traitement, plus grand est le risque de modifier, d'altérer, de transférer ou d'utiliser ces données à des fins étrangères.

Voilà pourquoi notre chambre ne partage pas l'approche du législateur consistant à centraliser et

harmoniser *à tout prix* les données d'identification des personnes dans un seul registre dont la simplification administrative pour les administrés et les administrations aura notamment pour contrepartie une désagrégation du contrôle de ces données par la CNPD et, par conséquent, une entrave aux libertés individuelles du citoyen.

En raison des observations formulées ci-dessus, notre chambre a le regret de vous communiquer qu'elle ne peut accueillir favorablement le projet de loi cité sous rubrique.

Luxembourg, le 27 mars 2009

Pour la Chambre des salariés,

La direction | Le président

René PIZZAFERRI | Norbert TREMUTH | Jean-Claude REDING

L'avis a été adopté à l'unanimité.