Avis de la Commission nationale pour la protection des données concernant le projet de loi n°5950 relatif à l'identification des personnes physiques, au registre national des personnes physiques et à la carte d'identité

Délibération n°48/2009 du 10 mars 2009

Conformément à l'article 32 paragraphe (3) lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée « la loi du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission d'aviser « *tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi* ».

C'est dans cette optique que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi n°5950 relatif à l'identification des personnes physiques, au registre national des personnes physiques et à la carte d'identité.

Elle constate à titre liminaire que le projet de loi sous examen ne comporte pas de modification en profondeur du système existant en matière d'identification numérique des personnes physiques, et ce malgré les problèmes soulevés en pratique ayant fait l'objet de discussions précédant le projet de modification de la législation actuelle.

Avant de proposer ses réflexions et propositions au sujet du projet de loi sous examen, la Commission nationale estime qu'il est nécessaire de rappeler les préoccupations et intérêts en cause dont le législateur se doit de tenir compte et plus particulièrement les exigences de droit communautaire en matière d'identification numérique des personnes physiques.

I. Introduction

Le projet de modification de la législation relative au numéro d'identification nationale des personnes est directement lié aux travaux effectués par le Comité National pour la Simplification Administrative en faveur des Entreprises (CNSAE).

Ce comité, créé en date du 16 décembre 2004 et coordonné par le Ministère des Classes Moyennes, du Tourisme et du Logement en collaboration avec le Ministère de l'Economie et du Commerce extérieur, a été mis en place dans le cadre de la mise en œuvre du programme gouvernemental du 4 août 2004[1].

Concomitamment à la création de ce comité, la Chambre des Métiers a élaboré deux rapports relatifs à la réduction des charges administratives[2] dans lesquels elle estime nécessaire la mise en place rapide d'une politique de simplification administrative.

[1] La ligne « Directrice Intégrée 14 » prévoit que « *le gouvernement accordera une priorité à la simplification des formalités qui freinent le rendement et l'esprit d'initiative des PME* »

[2] Réduction des charges administratives Perspectives d'une future politique de simplification administrative au Luxembourg, Centre de Promotion et de Recherche, décembre 2004

Le Conseil du Gouvernement a reçu du CNSAE une note du 31 mars 2006 intitulée « *identifiant unique* » qui suggère la révision de la loi du 30 mars 1979 instituant l'identification numérique des personnes. Suite à cette note, un groupe de travail interministériel ad hoc « *identifiant unique* » a vu le jour.

Par ailleurs, l'identification numérique a fait l'objet de plusieurs questions parlementaires.

Dans sa réponse du 12 juin 2006 à la question parlementaire du 4 juin 2006 No 1.056 posée par l'honorable députée Madame Colette Flesch[3], Monsieur le Ministre des Communications Jean-Louis SCHILTZ a affirmé ce qui suit :

> *« Des évolutions récentes montrent également que l'utilisation fréquente du numéro d'identité national dans les procédures et usages administratifs vient de diluer la ligne de démarcation entre les usages licites et non licites dudit numéro tel qu'elle avait été tracée par la loi de 1979.*
> *La généralisation de l'emploi du numéro d'identité national en pratique mérite aujourd'hui une réflexion profonde sur les conditions d'utilisation du numéro d'identité et du répertoire général des personnes ainsi que sur les garanties susceptibles de satisfaire aux exigences de protection de données de la personne concernée.*
> *C'est la raison pour laquelle le Gouvernement a instauré un groupe de travail chargé de se pencher sur cette question et de faire des propositions pour réviser la législation sur le répertoire général des personnes physiques et morale en général et l'utilisation du numéro d'identité en particulier ».*

Le CNSAE a remis son rapport « Entfesselungsplang fir Betriber » en février 2007.

Ce rapport a mis en exergue cinq préalables à la simplification administrative, l'un d'eux étant la mise en place d'un identifiant unique[4].

Ce rapport précise encore ce qui suit :

> *« L'identifiant numérique instauré par la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales et les pratiques administratives s'y attachant doit être revu. (…)*
> *Un nouveau système d'identification des personnes physiques et des entreprises répondant à la fois à la simplification administrative et aux exigences de protection des personnes à l'égard du traitement des données à caractère personnel s'avère nécessaire. (…)*
> *D'abord il faudra mettre une législation adéquate. Ensuite l'idée de créer un répertoire général des entreprises au sens large (entrepreneurs individuels, personnes morales, établissements publiques, ASBL, fondations etc.) et un répertoire distinct pour les personnes physiques a été approuvée par le Conseil en Gouvernement.[5] »*

Il ressort de ce qui précède que le groupe interministériel était confronté à deux problèmes potentiellement contradictoires.

D'une part, le gouvernement souhaitait parvenir à une simplification des démarches administratives.

Et d'autre part, il estimait qu'il était devenu nécessaire de proposer de nouvelles garanties en matière de protection de données car il constatait que les règles et

[3] Sur ce même thème, elle a également posé les questions parlementaires No 1.127, 1.128 en date du 20 juin 2006 et No 2.205 le 8 janvier 2008.

[4] CNSAE « Entfesselungsplang fir Betriber » Février 2007, page 34
[5] Id. page 77

principes de protection des données posés par la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales (ci-après : la loi du 30 mars 1979) étaient dépassés et n'étaient plus respectés. Dans son avis du 9 janvier 2004, la Commission nationale avait déjà développé cette problématique[6].

Dès lors, le groupe de travail interministériel précité avait pour mission de parvenir à une simplification administrative tout en y intégrant de nouvelles garanties en termes de protection des données.

La Commission nationale a été consultée périodiquement par ce groupe de travail.

Lors d'une première consultation, elle a suggéré au groupe de travail de se poser la question de savoir si la réforme allait ou non apporter une réponse à la demande croissante d'élargissement de l'utilisation de l'identifiant numérique au-delà du cercle restreint des administrations publiques actuellement autorisées par voie de règlement grand-ducal. Elle observait, en effet, que l'identifiant numérique était de plus en plus utilisé en dehors du cadre légal. Le groupe de travail a confirmé ceci car cet élargissement formait une demande réelle des acteurs du secteur privé.

La Commission nationale a alors donné à considérer que l'élargissement à certains acteurs privés de l'usage de l'identifiant unique pouvait s'envisager pour tenir compte de l'évolution de la société actuelle mais devait alors être accompagné de solutions novatrices en vue de renforcer les garanties robustes destinées à éviter des risques d'abus et cela au moyen de solutions technologiques modernes qui n'existaient pas lors de l'adoption de la législation actuelle.

La Commission nationale était bien consciente que la première direction proposée n'était pas envisageable ; en effet, les garanties prévues par la loi du 30 mars 1979 étaient cantonnées aux seules relations entre l'administré et les administrations. Par conséquent, l'élargissement du numéro d'identification à des acteurs du secteur privé devait conduire à rechercher une palette plus large des garanties juridiques et techniques encadrant l'utilisation et les flux de l'identifiant numérique.

La Commission nationale a donc plaidé pour une démarche audacieuse plutôt que frileuse et conservatrice et donc pour envisager la mise en place de garanties juridiques et technologiques nouvelles. Dans le cadre de pistes de réflexion, elle présentait les systèmes adoptés dans d'autres pays européens et qui donnaient satisfaction en termes de protection des données.

Elle ne peut donc cacher une certaine déception à la lecture du projet de loi sous examen alors qu'elle semble ne pas avoir été suivie au niveau de ses préconisations de s'inspirer des exemples d'autres pays et des dispositions visant à assurer les principes régissant la matière de la protection des données à caractère personnel.

[6] Délibération 2/2004 Avis au sujet de l'avant-projet de règlement grand-ducal concernant l'accès au répertoire général des personnes physiques et morales par les officiers publics et autres créateurs ou exécuteurs d'actes translatifs de propriété immobilière ou de constitution d'hypothèque

II. Préliminaires

Principes régissant la protection des données

Tous les pays européens n'ont pas mis en place un identifiant unique destiné à être utilisé à l'occasion de toutes les démarches administratives.

La constitution de certains pays interdit parfois l'utilisation d'un identifiant national multisectoriel unique[7].

En Allemagne, l'utilisation d'un tel identifiant n'est pas interdit formellement par la Constitution, mais le Bundestag a estimé que la Cour constitutionnelle d'Allemagne avait décidé dans son arrêt du 15 décembre 1983 [8] que l'utilisation d'un identifiant unique multisectoriel pouvait être inconstitutionnel[9].

Il est vrai que l'utilisation d'un identifiant unique présente certains avantages pratiques.

Ainsi, l'administration est en mesure de croiser des informations sur une personne pour vérifier l'exactitude de ses affirmations et parer aux éventuelles fraudes. Le Comité Lindop au Royaume-Uni mettait également en exergue le fait qu'avec « *un seul et unique identifiant le coût global pour l'utilisateur serait réduit. De même le citoyen n'aurait plus à se souvenir des divers identifiants, spécifique à chacune de ses nombreuses activités* »[10].

Mais la mise en place et l'utilisation d'un identifiant unique peut aussi présenter des risques au niveau des libertés et droits des citoyens.

En France, la Commission Nationale Informatique et Libertés (ci-après : la CNIL) a affirmé que « *l'utilisation généralisée d'un identifiant unique dans l'ensemble des fichiers, en ce qu'elle faciliterait leur interconnexion, permettrait de tracer les individus dans tous les actes de la vie courante* »[11].

C'est d'ailleurs suite à un projet concernant un identifiant national unique que la CNIL a été créée. En effet, vers 1974, les services du Ministère de l'Intérieur finalisaient un projet intitulé SAFARI (pour « Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus ») révélé par la presse. Ce projet prévoyait d'instituer un identifiant unique pour interconnecter tous les fichiers des administrations. La révélation de ce projet a suscité une vive émotion de l'opinion publique qui craignait un fichage général de la population. Face à cette protestation, le gouvernement avait alors institué une commission appelée « Commission Informatique et Libertés » auprès du Ministère de la Justice pour proposer des mesures garantissant le développement de l'informatique dans le respect de la vie privée, des libertés individuelles et des libertés publiques. Cette commission avait suggéré la création d'une autorité indépendante; le projet de loi y afférant a été examiné à la fin de l'année 1977 et la loi a été votée le 6 janvier 1978[12].

---

7 Par exemple, l'article 35 de la constitution au Portugal

8 Bundesverfassungsgericht BVerfGE 65, 1 – Volkszählung, "Volkszählungsurteil"

9 eID Interoperability for PEGS, National Profile Germany, November 2007, IDABC, page 9 http://ec.europa.eu/idabc/en/document/6485/5938

10 Rapport du Comité pour la protection des données 1978, chapitre 29 paragraphe 6

11 Echos des séances du 28 avril 2006

12 Loi No 78-17 relative à l'informatique, aux fichiers et aux libertés

Le danger majeur de l'utilisation d'un identifiant numérique multisectoriel est donc la possibilité de croiser les informations contenues dans divers fichiers et relatives à une même personne. C'est comme si on pouvait créer un puzzle sur une personne à partir des différents éléments contenus dans les divers fichiers grâce à une clé unique : les informations sont éparpillées dans les fichiers d'administrations distinctes poursuivant des activités et missions ayant des finalités différentes entre elles et ces informations sont toutes rassemblées – ou sont susceptibles de l'être – pour tout savoir sur le titulaire du numéro d'identification unique.

Cette idée a été traduite par le spectre de *Gläserner Bürger* : la personne est comme « *transparente* » aux yeux de tiers car toutes les informations qui la concernent sont susceptibles d'être disponibles.

De plus, les personnes peuvent avoir le sentiment d'être réduites à une suite de chiffres dans ses rapports avec l'administration, mettant ainsi de côté le rapport humain.

Enfin, il existe un risque réel de détournement de finalité : des personnes travaillant dans une administration autorisée à recourir au numéro d'identification seraient en mesure d'obtenir des informations personnelles sur des administrés alors que ces informations ne sont pas nécessaires et/ou utiles dans le cadre de leurs activités. La recherche d'informations pourrait être mue simplement par la curiosité. Pour d'aucuns, ce risque serait d'autant plus accru dans un pays de petite taille.

La Cour européenne des Droits de l'Homme a eu à se prononcer à plusieurs reprises sur l'identifiant unique[13].

Elle affirme que l'utilisation d'un identifiant unique peut dans certains cas entraîner la violation de l'article 8 de la Convention de sauvegarde européenne des Droits de l'Homme et des Libertés fondamentales.

Il est un fait que le principe de la mise en place et de l'utilisation d'un identifiant national unique et multisectoriel n'est pas interdit pas les normes internationales ou européennes.

A notre connaissance, le premier texte à s'être prononcé sur l'identifiant unique est la Recommandation (86)1 relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale adoptée par le Comité des Ministres du Conseil de l'Europe le 23 janvier 1986.

Cette recommandation rappelle d'abord ce qui suit :

> *« Un équilibre doit être trouvé entre la nécessité d'utiliser des données à caractère personnel dans le domaine de la sécurité sociale, d'une part, et, d'autre part, la nécessité d'assurer la protection de l'individu notamment lorsque les données font l'objet d'un traitement automatisé* ».

Dans son paragraphe 5, elle précise que :

> *« L'introduction ou l'utilisation d'un numéro de sécurité sociale uniforme et unique ou de tout autre moyen analogue d'identification devrait s'accompagner de garanties adéquates prévues par le droit interne. »*

[13] Par exemple, Lindquist c/ Suède 10879/84, Lundvall c/ Suède 10473/83 et Kolzer c/ Suède 11732/85

L'exposé des motifs annexé à la dite recommandation précise encore :

> *« 34. Un numéro de sécurité sociale peut faciliter l'interconnexion et la contre-vérification des dossiers, simplifiant ainsi considérablement l'exécution des tâches des institutions de sécurité sociale. Aux termes du paragraphe 5.1, le droit interne doit prévoir des garanties adéquates lorsqu'un Etat membre introduit un numéro de sécurité sociale uniforme et unique ou un moyen d'identification analogue ou en fait usage s'il existe en déjà. On estime que de telles garanties sont souhaitables compte tenu des craintes que suscitent les identifiants. On peut redouter, par exemple, que l'introduction d'un numéro de sécurité sociale permette à des autorités qui exercent leurs activités en dehors du secteur de la sécurité sociale de se servir de ce numéro à leurs propres fins. Ce qui a été conçu à l'origine comme un numéro délivré à une fin particulière pourrait rapidement devenir un numéro standard, bon pour tous les usages. Des soupçons peuvent aussi surgir à l'égard du type d'informations figurant sur les cartes d'identification dont la finalité est analogue au numéro de sécurité sociale.*
>
> *35. C'est pour parer à ces craintes et ces soupçons que le paragraphe 5.1 parle de la nécessité d'accompagner de garanties adéquates l'introduction et l'utilisation de numéros de sécurité sociale. L'introduction de numéro standard répondant à tous les besoins ne devrait pas se faire de manière clandestine. Il conviendrait également de prévoir des garanties à l'égard des informations figurant sur les cartes d'identification. Ces informations devraient, par exemple, être lisible et ne pas être excessives au regard de leur finalité ».*

La Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données (ci-après : la directive 95/46/CE), transposée en droit interne par la loi du 2 août 2002, se prononce également sur l'identifiant unique.

L'article 8 relatif aux « *traitements portant des catégories particulières de données* », communément appelées « *données sensibles* » dispose que :

> *« 7. Les États membres déterminent les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement. »*

Les conditions auxquelles la directive en question fait référence sont, sous une autre expression, les garanties appropriées exposées par le Conseil de l'Europe dans sa recommandation précitée.

Les limitations, les conditions ou garanties accompagnant la mise en place et l'utilisation des numéros d'identification peuvent revêtir différentes formes.

Le Conseil de l'Europe relève des aspects juridiques et techniques[14].

Concernant les garanties juridiques, il peut par exemple s'agir d'un formalisme préalable à l'utilisation du numéro d'identification. A titre d'exemple, au Danemark, l'identifiant national ne peut être enregistré par les organismes privés que si la loi le prévoit ou en cas d'autorisation expresse de la personne concernée. Actuellement au Luxembourg, une des garanties consiste dans l'exigence légale de l'autorisation par voie de règlement grand-ducal de toute utilisation du numéro d'identification.

Il peut également s'agir d'une condition (notamment dans l'autorisation par les comités sectoriels dans le régime belge) subordonnant le recours au numéro

[14] « Le numéro personnel d'identification : leur mise en œuvre, leur utilisation et la protection des données » Etude préparée par le Comité d'experts sur la protection des données en 1991

d'identification à des finalités clairement délimitées ainsi que d'une mesure pour parer à d'éventuels abus dans l'utilisation du dit numéro.

Quant aux garanties techniques, celles-ci doivent être suffisantes compte tenu des règles de l'art : si elles sont obsolètes ou dépassées, elles ne protègent plus. Ces garanties peuvent consister en la mise en place d'une journalisation des saisies et/ou des consultations et/ou des transmissions ou encore d'un historique d'utilisation, de cryptage informatique ou toute autre architecture complexe permettant de contrôler les flux d'utilisation du numéro.

Des systèmes qui offrent des garanties appropriées au niveau juridique et technique existent dans des pays européens : il est tout à fait possible à l'heure actuelle de parvenir à un équilibre entre la protection des données à caractère personnel et la simplification administrative tout en conservant un numéro d'identification unique multisectoriel.

Le meilleur exemple mis en place est celui qui existe en Autriche. D'autres systèmes proposent également des garanties significatives.

Exemples de systèmes existant dans des pays européens

Le système autrichien : un modèle conciliant parfaitement la protection des données avec l'efficacité administrative [15]

L'Autriche a mis en place un système de communication électronique sécurisé dans lequel la protection des données à caractère personnel est pleinement assurée.

L'identification des personnes physiques s'effectue à partir des enregistrements existant dans un registre de base (*Basisregister*) et avec un numéro d'identification de base (*Stammzahl).* Pour les personnes physiques, le Registre Central des Résidents est le plus important « *Zentrales Melderegister – ZMR* ».

Les registres contiennent un nombre nécessaire d'identifiants pour garantir que les personnes sont identifiées de manière fiable les unes par rapport aux autres.

Le nombre d'identification de base (*CRR- Central Residents Register* également appelé source-PIN) est généré à partir d'un nombre dérivé du numéro *ZMR – Ergänzungsregisterzahl* et d'une clé secrète qui est gardée par la Commission autrichienne de protection des données dans son rôle d'autorité du registre e-government. Le nombre CRR est exclusivement enregistré sur la « carte de citoyenneté » (*Bürgerkarte*) utilisée par son titulaire dans tous ses rapports avec les administrations.

Ce nombre CRR ne peut être traité qu'avec un logiciel sécurisé spécifique.

Il sert d'identifiant unique et remplit la fonction de source unique d'identification. Il est ainsi le point de départ pour la création des identités électroniques protégées.

En effet, dans les communications électroniques avec l'administration, les personnes physiques sont identifiées par un identifiant personnel sectoriel (ci-après : ssPIN). Ces ssPIN sont calculés en appliquant un procédé cryptographique sur la source-PIN et sur le secteur procédural spécifique à l'administration. Le

15 "Behörden im Netz. Das ¨sterreichische E-Government ABC " ainsi que "Best Practice Katalog. E-Government in Österreich", Bundeskanzleramt Österreich, éd. Digitales Österreich

ssPIN est différent pour chaque administration, de sorte qu'un ssPIN valide pour une autorité ne peut pas être employé pour obtenir des informations sur le titulaire du numéro par une autre administration.

En d'autres mots, les autorités publiques emploient différents identifiants personnels dérivés de la source-PIN de la personne physique et du secteur procédural considéré. La dérivation est basée sur une opération cryptographique irréversible, ce qui assure que la source-PIN ne peut pas être identifiée à partir de l'identifiant dérivé.

Les passerelles entre fichiers d'administrations différentes sont possibles grâce à une « plaque tournante informatique» par laquelle les flux de données sont tous contrôlés et tracés.

Les systèmes de gestion des données personnelles sont fortement encadrés par différents règlements, pour garantir un niveau de sécurité optimal tout en garantissant le flux de ces données entre les divers services de l'administration publique.

Ce modèle présente l'avantage indéniable de protéger pleinement les données des administrés car le système repose sur un numéro de référence unique qui arrive à brasser et à créer d'autres numéros qui sont seulement connus des administrations concernées. Ainsi, par exemple, à partir du numéro sectoriel qui lui est attribué, l'administration de la santé ne peut pas accéder aux données détenues par d'autres administrations : si, dans le cadre de la simplification des démarches administratives, elle souhaite obtenir une information d'un organisme de sécurité sociale, elle fait une demande qui transite par la « plaque tournante informatique». Toutes les opérations sont journalisées aux fins de vérification, de contrôles ultérieurs.

Il convient de noter que la carte de citoyenneté n'est pas seulement utilisée dans le cadre des relations de son titulaire avec les administrations publiques mais qu'elle sert également dans des applications mettant le citoyen en relation avec des acteurs privés comme les banques.

A défaut de la validation d'un échange de données, une administration ne peut avoir connaissance des données des citoyens contenues dans les fichiers des autres administrations.

Compte tenu de la parfaite adéquation entre le principe de protection des données et les principes de simplification et d'efficacité administratives, certains pays ont tenté d'importer ce modèle. Ainsi, le Préposé Fédéral suisse avait recommandé publiquement son adoption par la Confédération helvétique.

Même si le groupe de travail interministériel n'a pas retenu le modèle autrichien, probablement à cause de son degré de sophistication et de son coût économique, susceptible de dépasser le cadre approprié pour un pays de petite taille, la Commission nationale donne à considérer que ce système s'appuie sur des idées maîtresses intéressantes qui pourraient bel et bien être reprises au Luxembourg. Il est incontestable que ce système apporte une meilleure protection contre d'éventuels abus avec les données des citoyens.

Le système belge

La Belgique a mis en place un ensemble de mesures pour promouvoir la simplification administrative. D'ailleurs, depuis 1998, l'Agence pour la Simplification Administrative (ci-après : ASA) fait des propositions pour simplifier les obligations légales et les procédures administratives. L'ASA est rattachée à la Chancellerie du Premier Ministre et elle est dirigée par un comité d'orientation tripartite.

L'attribution d'un numéro unique aux personnes physiques et aux entreprises poursuit deux objectifs distincts à savoir 1) devenir un outil de la simplification administrative car les utilisateurs utilisent désormais un seul et même numéro au lieu et place des différents numéros sectoriels attribués par les administrations et, 2) la mise en place d'une clé d'identification unique pour échanger les données entre administrations et parvenir ainsi à une collecte unique des données[16].

Le système belge a développé le système des sources authentiques.

Une source authentique est une base de données fiables mise à la disposition de tiers autorisés. Lorsqu'une administration autorisée à consulter une ou des sources authentiques, elle ne peut plus demander ces mêmes données aux administrés.

Les données de différentes sources authentiques relatives à un domaine sont regroupées dans les banques-carrefours.

Ces banques-carrefours sont contrôlées par des comités sectoriels institués auprès de la Commission pour la protection de la vie privée.

Les comités sectoriels sont composés à part égale de membres de la dite Commission pour la protection de la vie privée et d'experts du secteur concerné. La présidence des comités revient en théorie au président de la Commission pour la protection de la vie privée. Lors des votes, la voix du président est prépondérante en cas de partage de voix[17]. De plus, le « *président recherche la position commune susceptible d'être adoptée* »[18].

Les comités sectoriels sont également chargés de délivrer les autorisations préalables d'accès et de communications des données se trouvant dans la banque-carrefour qu'ils sont chargés de surveiller. Pour ce faire, ils procèdent notamment à une analyse de la finalité recherchée et des mesures organisationnelles et techniques des opérations de traitement.

A l'heure actuelle, six comités sectoriels existent :

- le Comité sectoriel du Registre national. Il a été créé par la loi du 8 août 1983 organisant un registre national des personnes physiques. Il veille à la sécurité et à la protection des données enregistrées dans le registre national des personnes physiques et il contrôle l'utilisation du numéro d'identification nationale. Il accorde à ce titre les autorisations d'accès et de communications des données à des catégories de personnes préalablement déterminées par une loi, un décret ou une ordonnance et dans le cadre de leurs activités également délimitées[19].

16 ASA Guide de Simplification administrative, chapitre II : le Numéro unique – février 2008
17 Article 12 paragraphe 5 du Règlement d'ordre intérieur des Comités sectoriels
18 Id. article 12 paragraphe 3
19 Article 5 de la loi précitée du 8 août 1983

- le Comité sectoriel de la Banque-Carrefour des Entreprises a été créé par la loi du 16 janvier 2003 portant création d'une Banque Carrefour des Entreprises.

- le Comité sectoriel de la Sécurité Sociale et de la Santé, créé par la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale. Il veille à ce que les traitements de données à caractère personnel effectués dans le cadre des activités de sécurité sociale n'aient pas de répercussion sur la vie privée des assurés.

- le Comité sectoriel pour l'Autorité Fédérale, créé par une loi du 8 décembre 1992, surveille le flux électronique de données à caractère personnel au sein de l'administration fédérale.

- le Comité de surveillance sectoriel Phenix, créé par une loi du 10 août 2005, veille à la sécurité et à la confidentialité des traitements de données à caractère personnel effectués par l'appareil judiciaire belge.

- le Comité de surveillance statistique, créé par une loi du 4 juillet 1962, contrôle la communication par le Directeur général Statistique et information économique, de données codées à des tiers ainsi que leur utilisation par des tiers.

Le registre national des personnes physiques contient les données d'identification des résidents sur le territoire belge. Chaque personne reçoit un numéro d'identification personnel et unique. Ce numéro est composé de onze chiffres[20] : les six premiers correspondent à la date de naissance, les trois chiffres suivants sont des numéros d'ordre pour départager les personnes nées à la même date tout en prenant en compte que les hommes se voient attribuer un numéro impair et les femme un numéro pair ; les deux derniers chiffres forment un nombre de contrôle. Il est donc possible de retrouver des informations à caractère personnel sur les titulaires à partir de leur numéro d'identification.

L'utilisation du dit numéro d'identification est subordonnée à une autorisation préalable du Comité sectoriel du Registre national.

Les banques-carrefours mènent les échanges de données à caractère personnel entre les institutions qui ont été préalablement autorisées : par exemple, lorsqu'une institution a besoin de certaines données à caractère personnel pour l'exécution de ses missions, le répertoire des références effectuera automatiquement le routage de cette demande vers l'institution qui est la plus apte à mettre ces informations à disposition. Une réponse sera ensuite transmise à l'institution demanderesse.

Les données sont donc communiquées et échangées dans le cadre d'un réseau en étoile.

Ainsi, un contrôle préventif de la légitimité des échanges est mis en place car l'échange est effectué conformément à l'autorisation du Comité sectoriel concerné et selon les modalités prédécrites. Quand une personne autorisée a besoin de certaines données pour l'exécution de sa mission, elle est obligée d'adresser sa demande par voie électronique à la banque-carrefour.

De plus, toutes les demandes d'informations sont enregistrées par la banque-carrefour ou par l'organisme de gestion d'un réseau sectoriel afin de pouvoir

[20] Arrêté Royal du 6 novembre 2007 portant modification de l'Arrêté Royal du 3 avril 1984 portant sur la composition du numéro d'identification des personnes inscrites dans le Registre national des personnes physiques (Moniteur Belge 11 janvier 2008)

éventuellement tracer *a posteriori* tout détournement de finalité ou tout usage détourné des données sollicitées. Les banques-carrefours disposent ainsi de répertoire de référence pour retracer les échanges.

Ce système présente toutefois moins de garanties que le modèle autrichien.

La situation en Suisse

La législation relative au numéro d'identification national a été modifiée par loi fédérale sur l'assurance-vieillesse et survivants (LAVS) du 23 juin 2006 et mise en vigueur par le Conseil fédéral le 1er décembre 2007.

Avant l'entrée en vigueur de cette loi, le numéro d'identification était composé de onze chiffres et fournissait des informations sur son titulaire (date et lieu de naissance notamment). Ce système était très ressemblant à celui qui existe actuellement au Luxembourg.

Désormais, le numéro d'identification est composé de treize chiffres. De plus, il est non parlant et il est attribué de manière aléatoire.

La structure du numéro d'identification est inscrite dans la loi[21].

De plus, l'utilisation du dit numéro est encadrée : une loi doit autoriser au préalable son utilisation et doit identifier la finalité poursuivie ainsi que ses utilisateurs.

Il est utile de préciser que le nouveau numéro d'identification est utilisé depuis le 1er juillet 2008, soit environ une année et demie depuis l'entrée en vigueur de la loi du 23 juin 2006 précitée, ce qui démontre que la période de transition a été brève.

Malgré la mise en place rapide d'un numéro non parlant qui ne dévoile plus des informations personnelles, et tout en reconnaissant les améliorations par rapport au système antérieur, le Préposé Fédéral suisse à la protection des données a regretté que le système soit moins exigeant en matière de protection des données. Il regrette que la loi ne prévoit pas de mesure pour prévenir les interconnexions de données :

> *« (…) il ne suffisait pas de prévoir dans la loi l'utilisation d'un numéro non parlant pour garantir le respect de la protection des données. Il était indispensable de prévoir un modèle qui empêchait techniquement des interconnexions et des utilisations de données non autorisées et non nécessaires. Un tel modèle excluait de recourir au numéro d'assuré social comme clé d'accès à d'autres registres. Ce numéro devait ainsi être réservé au secteur des assurances sociales uniquement. L'objectif légitime et non contesté de l'harmonisation des registres, l'amélioration de l'outil statistique ou le développement de l'administration électronique pouvaient être réalisés sans recourir au numéro d'assuré social en tant qu'identifiant unique. A l'instar de notre voisin autrichien, il convenait d'étudier la mise en place d'un modèle basé sur des numéros sectoriels et une série de transformations cryptographiques à partir d'un numéro de référence unique attribué à chaque individu. (…) »*[22].

[21] Article 50c point 3

[22] Vers une société sous surveillance ? Jean-Philippe WALTER, Publications de l'EPFL, août 2006. http://ditwww.epfl.ch/SIC/SA/SPIP/Publications/spip.php?article1117

L'exemple du système français : les identifiants sectoriels et l'utilisation particulière du numéro d'inscription au répertoire national

Comme la Commission nationale le signalait précédemment, la France n'a pas recours à un identifiant national unique. Chaque secteur d'activité a recours à un identifiant sectoriel qui lui est propre.

Il existe un numéro d'inscription au répertoire national (ci-après : NIR) géré par l'INSEE, également appelé « numéro de sécurité sociale » car il est utilisé dans le secteur de la sécurité sociale. Ce numéro d'identification à treize chiffres est attribué à toute personne physique. Ce numéro est unique, deux personnes ne pouvant pas avoir le même numéro. Ce numéro est composé d'une série de caractères permettant de déterminer le sexe, la date et le lieu de naissance. Il est donc similaire dans sa composition et dans son utilisation initiale au numéro d'identification nationale luxembourgeois.

A notre connaissance, le NIR est utilisé dans un seul secteur en dehors du celui de la sécurité sociale à savoir dans le domaine fiscal : un amendement à la loi de finances pour 1999 du 18 novembre 1998 autorise en effet l'administration fiscale à utiliser le NIR dans un souci d'éviter les erreurs d'identité dans le cadre des échanges d'informations entre l'administration fiscale et les organismes sociaux. Le Conseil constitutionnel avait déclaré que cette utilisation du NIR était conforme à la constitution tout en y apportant des réserves d'interprétation car cette utilisation devait être assortie de plusieurs garanties, telles le secret professionnel renforcé et la circonscription de la finalité pour laquelle le numéro est utilisé[23].

La loi modifiée du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés contient également diverses dispositions en rapport avec le NIR.

Ainsi, l'article 27 dispose ce qui suit :

> *« I. Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'Informatique et des libertés :*
> *1° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public, qui portent sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques. »*

L'article 25 dispose encore :

> *« I. Sont mis en œuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 : (…)*
> *6° Les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription à celui-ci des personnes. »*

Ainsi, la CNIL a-t-elle un rôle important avant la mise en œuvre d'un traitement de données contenant le NIR et ce quand bien même ce numéro ne soit pas multisectoriel.

Dans le cadre de sa mission de contrôle, la CNIL admet que ce numéro soit utilisé dans l'ensemble des fichiers des organismes en relation avec ce secteur

[23] Décision du Conseil constitutionnel No 98-406 DC du 29 décembre 1998 relative à la loi de finances rectificative pour 1998

(employeurs, services de prestations chômage, organismes d'assurance maladie obligatoires et complémentaires santé, professionnels de santé) mais exclusivement dans leurs relations avec les organismes de sécurité sociale[24].

Elle refuse, par exemple, son utilisation par des organismes de recouvrement de créance ou des établissements de crédits[25] en considérant qu'au « *regard des risques présentés par la généralisation de l'usage du NIR et de l'application du principe de proportionnalité défini à l'article 6-3° de la loi du 6 janvier 1978, l'utilisation du NIR par un organisme n'intervenant pas dans le secteur de la sécurité sociale, ne pouvait être admise que si elle correspondait à la poursuite d'un besoin d'intérêt général* ».

Elle a encore précisé que « *la lutte contre la fraude ou l'homonymie sont des finalités qui, bien que légitimes, ne suffisent pas, à elles seules, pour justifier l'utilisation du NIR dans le cadre de gestion de produits d'épargne, de gestion de crédits ou encore de recouvrement de créance. (…) Les mutuelles, les entreprises d'assurances et les institutions de retraite complémentaire et de prévoyance sont autorisés à utiliser le NIR pour l'exercice de leurs activités d'assurance maladie, de maternité, d'invalidité complémentaires et d'assurance vieillesse mais non pour la gestion de la relation commerciale. Pour la gestion de ses relations commerciales, chaque organisme doit se doter d'un identifiant spécifique.* [26].

Elle a également affirmé que ce numéro ne pouvait pas servir d'identifiant spécifique du dossier médical[27].

**

Au vu des principes guidant la matière de la protection des données et tout en gardant à l'esprit l'intérêt de la simplification administrative, la Commission nationale se propose maintenant de présenter ses réflexions et commentaires au sujet de loi pré mentionné.

III. Examen du projet de loi N°5950

La Commission nationale entend limiter ses observations aux dispositions traitant des aspects de protection des données.

Elle rappelle qu'il n'est pas dans son intention que le principe d'un numéro d'identification uniforme et non équivoque soit abandonné en faveur de l'adoption d'un système reposant sur des numéros d'identification sectoriels. Elle s'est résolue à ne pas remettre en cause le recours à un numéro d'identification unique à utilisation multiple pratiqué depuis près de trente ans et qui, de plus, ne heurte plus guère la sensibilité de l'opinion publique.

Par contre, la nécessité de constituer des garanties qui se révèlent aujourd'hui défaillantes et/ou d'adjoindre des mesures de protection nouvelles mettant à profit notamment de nouveaux progrès techniques, nous semble indispensable alors que

[24] Conclusions de la Commission Nationale de l'Informatique et des Libertés sur l'utilisation du NIR comme identifiant de la santé, février 2007
[25] Autorisations du 23 février 2006
[26] Même référence
[27] Conclusions de la Commission Nationale de l'Informatique et des Libertés sur l'utilisation du NIR comme identifiant de la santé, février 2007

le projet de loi sous examen est sensé préparer une nouvelle ère de l'administration publique dans la société de l'information.

1. Le registre national des personnes physiques (article 1er, 5 et 6)

La vocation centrale d'un registre national des personnes physiques comprenant l'identifiant numérique des citoyens ne soulève pas de difficultés en soi.

1.1. Les données figurant dans le registre

La liste des données figurant dans le registre diffère quelque peu de celle qui existe actuellement dans le répertoire général des personnes prévu à l'article 3 paragraphe (2) de la loi du 31 mars 1979.

Ainsi, l'état civil ne figure plus dans le registre, le projet de loi évoquant désormais la situation de famille (article 6 paragraphe (2) lettre (e)). De plus, sont ajoutés les numéros d'identifications des pères et mères et/ou des enfants auprès de qui la filiation est établie. Le registre précise encore l'éventuel statut de réfugié ou de protection subsidiaire.

Il s'agit des données communes à toutes les administrations susceptibles de recourir au registre national : ces données permettent de donner une signalétique des personnes figurant dans le registre.

La Commission nationale estime que les données figurant dans le registre sont nécessaires et non excessives. Le catalogue des données est clairement circonscrit. Elle constate avec satisfaction qu'aucune donnée biométrique ne sera enregistrée dans ce registre.

Elle considère que le registre ne devrait pas contenir d'autres informations sur les titulaires des numéros d'identification nationale.

1.2. Le rôle du registre national

Le texte sous examen précise que le registre a pour finalité « *de regrouper toutes les données relatives à l'identification des personnes physiques, d'établir des statistiques et de préserver l'historique de ces données* »[28]. Il indique encore que le dit registre « *garantit la source authentique de certaines données enregistrées* »[29].

Les finalités sont larges car le registre est conçu pour répondre aux besoins d'administrations accomplissant des missions différentes. A l'instar du système belge, le registre assure la source authentique de données à caractère personnel, ce qui est conforme au principe selon lequel les données doivent être exactes, aux termes de l'article 4 paragraphe (1) lettre (c) de la loi du 2 août 2002.

2. Le choix de la structure de l'identifiant (article 2)

La Commission nationale relève tout d'abord que le texte sous examen ne donne pas de précision sur la nouvelle structure du numéro d'identification et qu'il faut se reporter à l'exposé des motifs pour obtenir quelques informations.

[28] Article 5 paragraphe (1)
[29] Article 5 paragraphe (2).

L'exposé des motifs précise que l'identifiant passe de onze à désormais treize chiffres. Dans un second temps, le numéro d'identification nationale serait non parlant. Il est encore précisé qu'un règlement grand-ducal sera pris à ces fins.

Il est regrettable que la loi ne fixe pas elle-même la structure envisagée, ni même ne mentionne qu'un règlement grand-ducal devra obligatoirement être pris à ces fins en termes de sécurité juridique. Il serait préférable que la loi le prévoit. La loi suisse précitée sur l'assurance vieillesse qui modifie la structure de l'identifiant unique précisait que ce dernier serait non parlant.

En l'absence de contrainte légale, le système actuel est susceptible de perdurer, avec les défauts et les insuffisances qui ont déjà été critiqués.

La Commission nationale regrette que les auteurs du projet de loi sous examen n'aient pas pris en compte le caractère singulier de l'identifiant unique en ce qu'il continue à contenir des informations à caractère personnel sur les personnes. Ces derniers envisagent certes la mise en place « *à terme* » d'un numéro aléatoire, c'est-à-dire non parlant, mais cette phase transitoire paraît, au vu des explications données dans l'exposé des motifs, particulièrement longue et excessive.

La Commission nationale n'est pas convaincue de la nécessité d'une phase transitoire avant la mise en place d'un système reposant sur un identifiant personnel non parlant, quand bien même la migration technique doit avoir lieu dans cinq ans. La Suisse avait un système similaire à celui qui existe au Luxembourg et elle n'a pas eu recours à une phase transitoire ; qui plus est, la mise en place des numéros non parlants est devenue effective un an et demie après l'entrée en vigueur de la loi qui l'instituait.

De plus, la double migration envisagée par les auteurs du projet de loi sous examen présente de nombreux désavantages. En sus de son coût financier significatif, les travaux de migration technique doivent être répétés avec le risque d'erreurs que cela peut engendrer. A cela s'ajoute que le citoyen risque de ne pas comprendre qu'il va recevoir deux numéros d'identification. Cette situation paraît être en contraction avec le principe de la simplification administrative.

3. <u>L'utilisation élargie du numéro d'identification nationale (article 3)</u>

Le texte de loi en projet énumère les catégories de personnes pouvant utiliser l'identifiant national, sans qu'il soit pour autant nécessaire, comme dans le système actuel, de prendre des règlements grand-ducaux d'application.

La Commission nationale n'est pas surprise de cet élargissement pour les raisons ci-avant exposées. Cette ouverture permet de régler des situations de fait qui existent actuellement sans cadre légal.

Elle note encore que l'énumération des catégories de personnes du secteur de la santé doit s'entendre comme étant restrictive. Tous les professionnels du secteur de la santé qui ne sont pas énumérés ne pourront donc pas utiliser le numéro d'identification.

Le projet de texte sous examen interdit dans le secteur privé l'utilisation du numéro d'identification comme clé de recherche et le fait de pouvoir continuer ce numéro à des tiers.

Toutefois, il ne prévoit pas de sanctions au non respect de cette disposition. A cela s'ajoute que cette interdiction est un leurre car, d'un point de vue technique, toute donnée peut servir de clé de recherche. Cette interdiction se trouve donc en décalage avec les réalités techniques actuelles.

Les abus actuellement constatés pourrait donc persister en l'absence de sanction prévue dans le texte.

Dès lors, la Commission nationale estime que la disposition relative à l'interdiction d'utilisation du numéro d'identification comme clé de recherche et le fait de le continuer à un tiers n'est pas une garantie suffisante du point de vue de la protection des données.

De plus, elle constate que le projet de loi indique une finalité pour recourir à l'utilisation de l'identifiant unique. Toutefois, cette finalité est si large qu'elle peut englober tout type de situation.

Il est vrai que la loi du 31 mars 1979 précisait déjà que le numéro était réservé à un usage administratif interne ou aux relations avec le titulaire du numéro ; mais les règlements grand-ducaux d'application donnaient toutes les précisions sur les administrations concernées, sur les documents et les actes en cause.

Le texte sous examen fait ainsi l'impasse sur le principe de finalité, principe pourtant cardinal en la matière de protection des données.

Cette situation est d'autant plus délicate que des acteurs du secteur privé peuvent désormais utiliser le numéro d'identification unique. La Commission nationale marque des réserves sur le libellé du paragraphe (4) relatif à l'utilisation de l'identifiant national dans le secteur privé : il peut être interprété de manière très large, de manière que toute personne pourrait justifier l'utilisation du dit numéro. Cela risque de conduire à la banalisation et à la divulgation incontrôlée du numéro d'identification.

En outre, le texte sous examen ne prévoit plus de contrôle *a priori* de l'utilisation du numéro d'identification.

Dans son rapport précité de 1991, le Conseil de l'Europe affirmait que « *la législation nationale à la protection des données doit expressément mentionner les garanties contre l'utilisation excessive des PIN* [numéros d'identification personnelle]».

Dans le système actuel, le traitement est apprécié lors de l'élaboration des règlements grand-ducaux d'application de la loi du 31 mars 1979.

Il aurait été souhaitable que le projet de loi sous examen prévoie des garanties au respect du principe de finalité.

A ce titre, la Commission nationale rappelle que le numéro d'identification nationale constitue une donnée à caractère personnel au sens de l'article 2 de la loi du 2 août

2002. Aux termes de son article 12, les traitements de données personnelles doivent être notifiés sauf dans les cas où la dite loi prévoit des exemptions de notification[30].

Lors de l'examen des notifications préalables, la Commission nationale sera en mesure de contrôler le respect des dispositions de l'article 6 paragraphe (1) lettre (b) de la directive précitée du 24 octobre 1995 aux termes duquel les données à caractère personnel doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités* ».

Par conséquent, et dans un souci de transparence et de sécurité juridique, la Commission nationale préconise l'ajout à la fin de l'article 3 d'un paragraphe additionnel rappelant l'obligation de notification de ces traitements.

4. La problématique du traçage des éventuels échanges de données entre les personnes autorisées à utiliser le numéro d'identification nationale

Bien que l'échange de données entre les administrations détenant l'identifiant unique n'ait pas été abordé dans le projet de loi sous examen, ni même dans l'exposé de ses motifs, la Commission nationale entend présenter les observations qui suivent.

La possibilité d'échanger des informations entre administrations au moyen du numéro d'identification surgit en filigrane de la volonté de parvenir à la simplification et à l'efficacité administrative. Dans son rapport, la CNSAE évoque d'ailleurs les échanges et partages des données entre les administrations gouvernementales[31].

La Commission nationale est d'avis que de tels échanges respectivement interconnexions ne sont pas interdits en soi, mais ne devront s'opérer que dans le respect de garanties techniques et juridiques solides inscrites dans la loi.

Ainsi il faut souligner que certains pays qui ont mis en place des cadres légaux facilitant l'échange respectivement les interconnexions de fichiers entre administrations ont également prévu des garanties techniques et légales.

En Autriche tous les échanges respectivement les interconnexions de fichiers entre administrations passent par une 'plaque tournante' centrale et sont contrôlés, autorisés et journalisés par l'autorité de protection des données.

En Belgique l'utilisation du numéro d'identification est subordonnée à une autorisation préalable du Comité sectoriel du Registre national. Les échanges respectivement interconnexions de fichiers entre administrations sont effectués à travers les différentes banques-carrefours et seront soumis à l'autorisation du Comité sectoriel concerné. Les banques-carrefours disposent d'un répertoire de référence pour retracer les échanges.

Au Luxembourg, de tels échanges respectivement interconnexions doivent expressément être prévus par un texte légal ou réglementaire, sinon faire l'objet d'une autorisation préalable de la Commission nationale.

[30] Ne sont pas non plus soumis à notification les traitements qui relèvent des dispositions prévues aux articles 8, 14 et 17 de la loi (article 12 paragraphe (1) lettre (a))

[31] Par exemple, point 2.3.7. du rapport Entfesselungsplang fir Betriber précité

Les textes légaux ou réglementaires autorisant une interconnexion de données doivent respecter le *ratio* des dispositions de l'article 16 de la loi du 2 août 2002[32]. Conformément à son paragraphe (1), l'interconnexion peut valablement être autorisée par voie légale.

Son paragraphe (3) traite des finalités des traitements interconnectés. Le paragraphe (2) pose quatre conditions cumulatives supplémentaires à savoir 1) des objectifs légaux ou statuaires présentant un intérêt légitime pour les responsables du traitement, 2) le fait de ne pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées, 3) la mise en place de sécurité appropriée et 4) la qualité des données faisant l'objet de l'interconnexion.

En vertu du paragraphe (3) de l'article 16 de la loi du 2 août 2002, les finalités des fichiers interconnectés doivent être compatibles entre elles. La notion de « compatibilité » n'est pas définie par la loi. Le critère de compatibilité est lié à l'un des principes majeurs de la législation de protection des données, à savoir la transparence des traitements de données à l'égard des personnes concernées par les données[33]. Ce critère est traditionnellement interprété comme signifiant prévisible par les personnes concernées, cette prévisibilité pouvant d'ailleurs naître seulement postérieurement à la collecte des données, par exemple par le seul fait d'une disposition légale ou réglementaire prévoyant l'utilisation ultérieure des données pour une finalité nouvelle.

Ensuite, l'objectif recherché par la personne qui accède aux fichiers d'un autre responsable du traitement doit être inscrit, soit dans la loi, soit dans ses statuts.

En vertu du principe selon lequel l'interconnexion ne doit pas conduire à une discrimination ou une réduction des droits, libertés et garanties pour les personnes concernées, la balance entre les intérêts des responsables du traitement et les intérêts des personnes concernées doit être maintenue en équilibre. En d'autres mots, si l'interconnexion permet d'obtenir par des moyens simples et rapides des informations sur une personne, cela ne doit pas se faire au détriment de ses droits et libertés. L'interconnexion doit dès lors être nécessaire pour atteindre la finalité poursuivie. De plus, le recours aux fichiers interconnectés doit être justifié.

Le droit de la protection des données s'appuie sur l'idée fondamentale que le responsable du traitement doit s'assurer que les données à caractère personnel qu'il détient soient traitées loyalement et licitement et ne soient pas ultérieurement traitées de manière incompatible avec les finalités déterminées et légitimes pour lesquelles il les a initialement collectées ou obtenues. En particulier, il doit s'en assurer lorsqu'il communique ces données à des destinataires ou lorsque des personnes placées sous son autorité directe sont habilitées à traiter les données. Il a également l'obligation de mettre en œuvre toutes les mesures techniques et l'organisation appropriées pour assurer la sécurité des traitements.

Conformément au vues du Conseil d'Etat le cadre légal luxembourgeois considère l'interconnexion de données comme une opération délicate qui doit être entourée d'un maximum de garanties[34]. Toutefois l'absence d'une 'plateforme centrale' comme celles des systèmes autrichien ou belge ne facilite par un contrôle à postériori des échanges des données effectuées.

---

[32] Documents parlementaires N° 4735/13, page 30

[33] « La Protection de la vie privée dans la société de l'information », Tomes 3 à 5, Chapitre 4, Cécile de Terwangne, pages 91 et suivantes, éd. Presse Universitaires de France, Cahier des sciences morales et politiques

[34] Avis du Conseil d'Etat du 30 janvier 2007 relatif au projet de loi n°5554

5. Quant au droit d'accès à l'historique de consultation du registre national des personnes physiques

La Commission nationale est satisfaite de la mise en place d'une journalisation des consultations du registre national des personnes physiques.

Elle s'interroge toutefois de l'intérêt pratique de cette garantie technique : en effet, le registre en question ne contient que la signalétique des individus. Si des administrations veulent s'échanger entre elles des informations sur les administrés autres que les données d'identification, elles ne vont pas consulter le registre national des personnes physiques.

6. La Commission du registre national (article 12)

L'article 12 *in fine* du projet de loi sous examen dispose qu'un règlement grand-ducal « *peut être pris pour déterminer la composition et le fonctionnement de la commission* ».

La Commission nationale estime que la composition et le fonctionnement de cette commission sont d'une importance majeure. Elle suggère que le projet de loi sous examen pose les lignes directrices de sa composition et de son fonctionnement, respectivement qu'un règlement grand-ducal soit effectivement pris concomitamment avec la loi sinon dans un délai particulièrement rapproché.

Elle se propose, par ailleurs, de participer à cette commission et d'y jouer une influence suffisante pour contrôler et apprécier le fonctionnement du registre national des personnes physiques à l'aune des principes de protection de données. A l'instar des comités sectoriels belges, cette influence peut se traduire par l'attribution d'un droit de vote prépondérant lors des séances de vote.

7. Quant aux données biométriques nécessaires à l'établissement des cartes d'identité

La Commission nationale marque sa satisfaction au fait que les données biométriques ne figureront pas dans des bases de données centralisées, elles sont uniquement conservées à titre préventif pendant les deux mois qui suivent la délivrance de la carte d'identité.

Cette conservation est nécessaire et justifiée.

Elle note également qu'aucune empreinte digitale ne sera collectée dans le cadre de la confection des cartes d'identité.

L'article 24 paragraphe (2) du texte sous examen précise qu'un règlement grand-ducal « *peut déterminer les normes et les simplifications techniques et fonctionnelles auxquelles doivent satisfaire les appareils et les applications qui rendent possible la lecture et la mise à jour des données prises de manière électronique dans la carte d'identité* ».

La Commission nationale est d'avis que ce règlement grand-ducal devrait être pris en même temps que la loi. Il est en effet primordial que des mesures de sécurité technique et technologique soient prises pour protéger les données insérées dans la carte à puce, et notamment le numéro d'identification nationale.

Comme pour les passeports biométriques, la puce qui sera contenue dans la carte d'identité pourra être lue à distance. Il existe en théorie un risque de lecture cachée des informations de cette carte à puce.

Le règlement (CE) 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyages contraint les États membres à instaurer des normes de sécurisation pour la lecture de la carte à puce.

Il serait nécessaire que ces normes de sécurisation soient également arrêtées avant la délivrance des premières cartes d'identité soit dans un règlement grand-ducal, comme l'envisage le texte sous examen, soit dans le corps même du texte du projet de loi sous examen afin de leur donner une valeur contraignante.

Ainsi décidé à Luxembourg en date du 10 mars 2009.

La Commission nationale pour la protection des données

Gérard Lommel Président	Pierre Weimerskirch Membre effectif	Thierry Lallemang Membre effectif