COMMISSION NATIONALE
POUR LA PROTECTION
DES DONNÉES

Rapport relatif aux Années 2004 à 2006

M. le Ministre Jean-Louis SCHILTZ, M. Gérard LOMMEL *(Président)*, M. Thierry LALLEMANG *(membre effectif)*, M. Pierre WEIMERSKIRCH *(membre effectif)*.
Photo prise lors de l'assermentation de M. Thierry LALLEMANG le 18 octobre 2005.

Table des matières

I Introduction

Vous avez dit, protection des données ?

Dans le prolongement de l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, la loi assure aux personnes physiques des droits tendant à voir protéger leur vie privée et impose des obligations aux acteurs qui opèrent des traitements de données comportant toutes formes d'informations relatives aux personnes qui sont susceptibles d'influencer la manière dont ils sont traités.

Cette protection s'étend même aux informations relatives à des personnes morales en vue de préserver leurs intérêts légalement protégés.

Les principes de la protection des données à caractère personnel sont repris dans la Charte des droits fondamentaux de l'Union Européenne (article II-8 de la future Constitution européenne) proclamée au Conseil européen à Nice.

Pour respecter la protection voulue par le législateur, les responsables de traitements de données sont obligés :

- de n'obtenir, stocker, utiliser et transmettre des informations concernant des personnes individuelles que loyalement et que pour des finalités déterminées, explicites et légitimes
- de ne pas les utiliser ou les partager avec des tiers, de manière incompatible avec ces finalités
- de s'assurer qu'elles sont adéquates, pertinentes et non excessives
- de prendre les mesures raisonnables nécessaires pour les maintenir à jour et éviter qu'elles soient inexactes ou incomplètes
- d'assurer leur confidentialité et sécurité (y compris à l'occasion de traitements effectués par des subordonnés et des sous-traitants)
- de ne pas les conserver plus longtemps que nécessaire, voire de les rendre anonymes si cela suffit
- de notifier les traitements de données à la Commission nationale, respectivement de solliciter leur autorisation préalablement à leur mise en œuvre dans les cas (comportant des risques particuliers) prévus par la loi
- de ne pas transférer des données à caractère personnel vers des pays hors Union européenne n'offrant pas un niveau de protection adéquat, sauf consentement des personnes concernées, autre dérogation légale ou garanties suffisantes résultant notamment de l'usage de clauses contractuelles appropriées validées par la Commission européenne ou d'autres mesures reconnues suffisantes par décision d'autorisation de la Commission nationale

Droits des personnes garantis par la loi du 2 août 2002 et la directive européenne 95/46/CE

- de voir des informations les concernant n'être traitées que loyalement et pour une cause légitime prévue par la loi
- d'être dûment informé dès la collecte des données, leur enregistrement, usage et la communication à d'autres par le professionnel ou l'organisation qui y procède auprès de qui davantage de renseignements peuvent être obtenus, notamment
- d'obtenir accès aux informations stockées et utilisées les concernant (copie)
- d'obtenir que des données inexactes soient corrigées et que les données non pertinentes ou excessives, eu égard à la finalité poursuivie, soient effacées

- de s'opposer à ce que des informations le concernant fassent l'objet d'un traitement s'il peut invoquer des raisons prépondérantes et légitimes tenant à sa situation personnelle ou bien si le traitement en question poursuit des fins de prospection (commerciale ou pour des motifs idéologiques)
- de voir toute utilisation de données les concernant s'arrêter lorsqu'il n'y a plus de raison nécessitant la poursuite du traitement en considération de la finalité initiale de ce dernier. En tout état de cause une utilisation à des fins autres que celle pour laquelle les données ont été collectées incompatibles avec cette finalité initiale n'est possible que moyennant un consentement préalable afférent et l'autorisation de la Commission nationale
- de demander à la Commission nationale pour la protection des données de vérifier la licéité d'un traitement de données personnelles et de pouvoir se plaindre auprès d'elle en vue de faire respecter la loi
- le cas échéant, de saisir la justice des atteintes illicites à leur vie privée et de réclamer réparation du dommage qu'ils auront éventuellement subi

Pour surveiller l'application de la loi une autorité de contrôle indépendante a été instituée qui intervient également pour informer le public, émettre des avis et traiter les plaintes.

Aux termes de l'article 28 de la directive et du protocole additionnel à la Convention 108 du Conseil de l'Europe chaque Etat membre/signataire doit mettre en place une autorité indépendante chargée de surveiller l'application de la loi sur la protection des données, d'être consultée dans le cadre du processus législatif et réglementaire pour toutes questions dans ce domaine et d'intervenir par des examens a priori et des contrôles a posteriori.

« Art. 32. Missions et pouvoirs de la Commission nationale »
(Extrait de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel)

(1) Il est institué une autorité de contrôle dénommée "Commission nationale pour la protection des données" chargée de contrôler et de vérifier si les données soumises à un traitement sont traitées en conformité avec les dispositions de la présente loi et de ses règlements d'exécution.

(2) Tous les ans, la Commission nationale rend compte, dans son rapport écrit aux membres du Gouvernement en conseil, de l'exécution de ses missions. Dans ce rapport, elle relève plus particulièrement l'état des notifications et des autorisations, les déficiences ou abus qui ne sont pas spécifiquement visés par les dispositions légales, réglementaires et administratives existantes. Elle publiera son rapport annuel. Le rapport est avisé par la commission consultative des droits de l'homme, organe consultatif du gouvernement en matière de droits de l'homme sur le territoire du Grand-Duché de Luxembourg dont la composition et les attributions sont déterminées par règlement grand-ducal.

(3) Les missions de la Commission nationale sont les suivantes:

(a) assurer l'application des dispositions de la présente loi et de ses règlements d'exécution en particulier celles relatives à la confidentialité et à la sécurité des traitements.

(b) recevoir les notifications préalables à la mise en œuvre d'un traitement, de même que les changements affectant le contenu de ces notifications, et procéder a posteriori au contrôle de la licéité des traitements notifiés; de même elle est informée sans délai de tout traitement soumis à autorisation préalable.

(c) assurer la publicité des traitements lui notifiés en tenant un registre afférent, sauf disposition contraire.

(d) autoriser la mise en œuvre des traitements soumis au régime de l'article 14 de la présente loi.

(e) être demandée en son avis sur 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. Ces avis sont publiés au rapport annuel visé à l'article 15, paragraphe 6.

(f) présenter au Gouvernement toutes suggestions susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données.

(g) recevoir et le cas échéant après discussion avec les auteurs approuver les codes de conduite relatifs à un traitement ou un ensemble de traitements lui soumis par des associations professionnelles représentatives de responsables du traitement;

(h) conseiller le Gouvernement, soit à la demande de celui-ci, soit sur sa propre initiative, au sujet des conséquences de l'évolution des technologies de traitement de l'information au regard du respect des libertés et droits fondamentaux des personnes; à cette fin, elle peut faire procéder à des études, des enquêtes ou expertises.

(i) favoriser de façon régulière et par tout moyen qu'elle juge opportun, la diffusion d'informations relatives aux droits des personnes concernées et aux obligations des responsables du traitement, notamment en ce qui concerne le transfert de données vers des pays tiers.

(4) La Commission nationale peut être saisie par toute personne, agissant par elle même, par l'entremise de son avocat ou par toute autre personne physique ou morale dûment mandatée, d'une demande relative au respect de ses droits et libertés fondamentaux à l'égard d'un traitement. La personne concernée est informée des suites réservées à sa requête.

(5) La Commission nationale peut, en particulier, être saisie par toute personne concernée d'une demande de vérification de la licéité d'un traitement en cas de refus ou de limitation de l'exercice du droit d'accès de la personne concernée conformément à l'article 29, paragraphe (4), de la présente loi.

(6) Si la Commission nationale est saisie par l'une des personnes ou organes visés à l'article 11, paragraphe (2), sur une violation de cet article, elle statue dans le mois de la saisine.

(7) Dans le cadre de la présente loi, la Commission nationale dispose d'un pouvoir d'investigation en vertu duquel elle a accès aux données faisant l'objet du traitement en question. Elle recueille toutes les informations nécessaires à l'accomplissement de sa mission de contrôle. A cette fin elle a un accès direct aux locaux autres que les locaux d'habitation où a lieu le traitement ainsi qu'aux données faisant l'objet du traitement et procède aux vérifications nécessaires.

(8) La Commission nationale a le droit d'ester en justice dans l'intérêt de la présente loi et de ses règlements d'exécution. Elle dénonce aux autorités judiciaires les infractions dont elle a connaissance.

(9) La Commission nationale coopère avec ses homologues que sont les autorités de contrôle instituées dans les autres Etats membres de l'Union européenne, dans la mesure nécessaire à l'accomplissement de leurs missions notamment en échangeant toutes informations utiles.

(10) La Commission nationale représente le Luxembourg au "groupe de protection des personnes à l'égard du traitement des données à caractère personnel" institué par l'article 29 de la Directive 95/46/CE.»

II Rapport d'activités

1. Activités de la CNPD

1.1 Activités en 2004

Les activités de la Commission nationale au cours de sa deuxième année civile étaient concentrées autour de plusieurs axes :

- Les formalités administratives : la réception et le traitement des déclarations effectuées dans le cadre des formalités préalables prévues au chapitre III de la loi.
- La mise en place de nombreux instruments de communication, d'information et de sensibilisation : prises de contact, séminaires, conférences, formations, interviews, édition de brochures d'information en collaboration avec le Service Information et Presse du gouvernement, développement du site Internet.
- L'information et la guidance des responsables du traitement et des contacts suivis avec les organisations représentatives sectorielles et les principaux acteurs devant se mettre en conformité avec les dispositions légales.

Des séances d'informations spécifiques ont eu lieu en collaboration notamment avec l'ordre des Experts comptables et la Chambre des Réviseurs d'entreprise, l'ISACA et l'IACI, l'Entente des hôpitaux, la COPAS et l'EGCA, des sociétés de sécurité, de gardiennage et d'installation d'équipements de surveillance.

Deux workshops ont été organisés par la Commission nationale pour la protection des données elle-même, l'un au CRP-Henri Tudor (Schlassgoart /Esch-sur-Alzette) et l'autre au Centre de Formation de la Chambre de Commerce. Des formations spécifiques furent également proposées par la Chambre des Employés Privés et l'Ecole Supérieure du Travail.

D'autres points importants dans l'activité de la Commission nationale en 2004 méritent d'être relevés :

- Dans son avis (délibération n° 2/2004 du 9 janvier 2004) relatif à 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, la Commission nationale pour la protection des données a rendu le gouvernement attentif à la nécessité de réviser la loi du 30 mars 1979 relatif au répertoire général des personnes. En effet la directive 95/46/CE (protection des données) prévoit en son article 8 § 7 que les conditions dans lesquelles un numéro national d'identification peut fixer l'objet d'un traitement devant être déterminées par la loi (garanties appropriées), car les garanties prévues par la loi du 30 mars 1979 ne se trouvent plus respectées en pratique, dès lors que le numéro de matricule des citoyens sont rendus publics (accessible par exemple au registre des hypothèques) ou communiqués à des tiers ou intermédiaires, comme certaines formalités le prévoient désormais.
- La délibération n° 3/2004 du 20 février 2004, suivant laquelle la Commission nationale a donné son avis à l'égard du projet de loi n° 5181 relatif aux dispositions spécifiques de protection des personnes à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification de la loi du 2 août 2002.
- La délibération n° 74/2004 du 13 septembre 2004 à l'égard de la loi du 6 juillet 2004 modifiant la loi du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques.
- L'avis de la Commission à l'égard du projet de loi n° 5356 relatif aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle (délibération n° 78/2004 du 8 octobre 2004) a suscité des réactions controversées dans les milieux judiciaires, politiques et dans la presse.

- L'appréciation portée sur les conditions et modalités de prélèvement, fichages et consultation de profils ADN des suspects, victimes, témoins, mais aussi des prévenus et personnes condamnés par la justice, se voulait toutefois pondérée et nuancée. Elle se fondait, pour l'essentiel, sur les orientations retenues en France et en Belgique (ou du moins sur les recommandations afférentes formulées par nos homologues) et sur les principes d'application de la Convention 108 aux traitements de données policières et judiciaires tels que dégagés dans les travaux du Conseil de l'Europe.
- La perspective de simplification de la loi qui implique deux types d'allégements des formalités à charge des responsables de traitements de données:
    - L'exemption de notifications pour les traitements les plus courants dès lors qu'ils ne comportent normalement pas de réserves pour l'incursion dans la vie privée.
    - La restriction plus poussée des traitements soumis à autorisation : Un certain nombre de cas de figure ne donnerait plus lieu qu'à notification (contrôle a posteriori de la Commission nationale au lieu d'un contrôle a priori sur dossier).
- La publication de plusieurs règlements grand-ducaux en application de la loi sur la protection des personnes à l'égard du traitement des données à caractère personnel, concernant notamment le rôle des chargés à la protection des données, les conditions applicables aux données à caractère personnel traitées par certains professionnels de la santé, l'accès de la police et des services d'urgence aux numéros de téléphone et adresses ainsi que le traitement par la police de données à caractère personnel en vue de l'application de la loi.
- La Commission nationale a publié un communiqué de presse pour clarifier l'application des dispositions de la loi aux tests génétiques de paternité à la suite d'un débat public sur ce sujet en République fédérale d'Allemagne qui a reçu également une large couverture dans les médias luxembourgeois.
- La prolifération de la vidéosurveillance, notamment pour sécuriser les espaces publics, la surveillance sur le lieu de travail opérée par l'employeur et l'utilisation des profils de clients dans les nouvelles techniques de marketing et de prospection agressive continuent d'être des sujets d'actualité commentés par la presse.
- A noter qu'un projet de loi a été déposé le 4 mars 2004 au Parlement en vue de la ratification du Protocole additionnel de la Convention 108 du Conseil de l'Europe (ETS n°181) qui comporte des dispositions nouvelles concernant les autorités de contrôle et les flux de données transfrontaliers.

Au niveau de la jurisprudence, il n'y a toujours pas de décisions significatives des juridictions judiciaires à signaler concernant l'application de la loi sur la protection des données, aussi bien dans les affaires civiles que pénales.

Néanmoins, le jugement du 15 décembre 2004 du tribunal administratif a retenu l'attention en ce qu'il a rejeté la requête en annulation d'une décision de la Commission nationale pour la protection des données, interdisant la vidéosurveillance des employés d'une chaîne de points de vente de duplication de clés et de cordonnerie. La Cour d'appel a confirmé la décision en juillet 2005 et a reconnu comme non fondés les griefs soulevés par l'employeur quant à l'interprétation de la loi faite par la Commission nationale pour la protection des données concernant l'application des principes de nécessité et de proportionnalité dans l'appréciation de la licéité des traitements de données soumis à son examen préalable.

1.2 Activités en 2005

Au début de l'année fut publiée la première liste de personnes agréées pour remplir la fonction de « chargé de la protection des données » propre à une entreprise, une organisation ou un établissement (article 40 de la loi), suite à l'intervention des dispositions réglementaires afférentes en décembre 2004.

La Commission nationale a d'ailleurs organisé un séminaire à leur intention le 3 juillet 2005 dans les locaux de la Chambre de Commerce avec une trentaine de participants.

L'activité de la Commission nationale au cours de l'année 2005 a été marquée par :

- L'accompagnement de l'élaboration du projet de révision de la loi (à la demande du Ministre de tutelle).

La Commission nationale a fait part au Ministre et à ses collaborateurs des constats qu'elle a dégagé de l'expérience de ses deux premières années d'activité et lui a soumis un certain nombre de propositions de modifications à apporter au texte dans l'optique de clarification et de simplification de la loi retenue dans le programme gouvernemental.

- Les objectifs du projet de révision de la loi ont d'ailleurs fait l'objet d'un débat nourri au sein du Comité national pour la simplification administrative en faveur des entreprises où le Président a exposé les vues de la Commission nationale et a répondu aux questions des représentants du patronat et des administrations publiques lors des réunions des 21 février et 20 juin 2005.
- Déménagement de ses bureaux vers le 41, avenue de la Gare à Luxembourg pour une phase transitoire avant son implantation définitive sur le site des friches industrielles de Belval-Ouest.
- Le traitement d'un grand nombre de formalités préalables à la mise en œuvre accomplies par les responsables en application du chapitre III de la loi.
- Les efforts déployés pour en optimiser la procédure et la prise en charge.
- L'élaboration d'un nouveau formulaire électronique interactif de notification intégrant les versions allemande et française, la notification ordinaire et simplifiée, les lexiques et le guide d'utilisation.
- La mise en ligne du registre public des traitements.
- Le lancement d'un audit des mesures de sécurité des données auprès du Centre Commun de la Sécurité Sociale, de l'UCM, des Caisses de Maladie et d'autres organismes de sécurité sociale.
- La relance du site Internet www.cnpd.lu (hébergé désormais auprès du CIE) avec un contenu plus étoffé et une présentation plus attractive au début du mois de septembre 2005. Celui-ci a été désigné « site Web du mois » par le magazine économique et financier Paperjam.
- Le changement intervenu dans la composition de la Commission nationale après le départ de M. Edouard Delosch (3 juillet) et la nomination de M. Thierry Lallemang en tant que membre effectif (le 18 octobre). Le service juridique au sein duquel officiait M. Lallemang en tant qu'unique juriste-employé s'en trouvait affaibli malgré le recours à deux nouveaux avocats qui collaborent depuis lors avec la Commission nationale par des prestations ponctuelles.
- La poursuite de sa campagne d'information du public notamment à travers diverses séances d'informations et la publication en partenariat avec l'Union Luxembourgeoise des Consommateurs du calendrier ULC 2006 entièrement dédié à la protection des données.
- L'édition de la brochure d'information de la CNPD en langue portugaise en décembre 2005.
- La participation à la conférence sur la sécurité dans les espaces publics, organisée par le Forum luxembourgeois pour la prévention et la sécurité urbaine (FLPSU) et parrainé par le Syndicat des villes et communes luxembourgeoises (SYVICOL) en octobre 2005. Les projets d'installation de systèmes de vidéosurveillance à l'initiative des élus locaux en vue d'améliorer la sécurité publique y ont été abordés.
- Signalons finalement l'avis rendu le 4 mai 2005 concernant un avant-projet de loi relatif à l'accès des officiers de police judiciaire à certains traitements de données à caractère personnel des personnes morales de droit public qui a entretemps donné lieu au projet de loi N°5563 déposé le 5 avril 2006 à la Chambre des Députés par le Ministre de la Justice.

Si les demandes d'autorisation examinées portaient pour l'essentiel sur des traitements à des fins de surveillance (vidéosurveillance, contrôle d'accès, surveillance des communications électroniques) ou de données sensibles ou relatives à la santé, l'étude des développements technologiques récents et les enjeux nouveaux afférents ont retenu de plus en plus l'attention des membres de la Commission nationale, notamment :

  - La biométrie à l'exemple du contrôle d'accès par authentification des empreintes digitales des abonnés par le domaine thermal de Mondorf
  - Les étiquettes électroniques à radiofréquence RFID
  - Les dispositifs d'alertes au sein des entreprises ou « whistleblowing » .

- La mise en œuvre de la surveillance par l'employeur sur le lieu de travail appliquée aux communications électroniques et à l'utilisation d'Internet et de la messagerie électronique, question qui donnait lieu à une décision de principe (Odyssey) rendue le 11 juillet 2005 qui fut publiée sur le site Internet de la Commission nationale (www.cnpd.lu), parce qu'elle constitue un cas d'espèce intéressant et reflète clairement les critères et conditions posés en application des articles 4 de la loi du 2 août 2002 et L.251-1 du Code du travail (ancien article 11 de la loi du 2 août 2002) pour l'autorisation d'une telle surveillance par l'employeur à l'égard de son personnel sur le lieu du travail. Il y a lieu de noter que de plus en plus de demandes sont introduites en vue de l'autorisation de tels traitements de données personnels par les employeurs.
- La Commission nationale pour la protection des données a pris sa première décision dans une affaire de biométrie. La Commission a refusé d'autoriser l'utilisation d'un système biométrique pour contrôler l'accès à un centre de fitness et de bien-être, alors que les données biométriques étaient stockées dans une base de données centralisée.
- Dans une autre affaire, la Commission nationale a été amenée à ne pas accorder l'autorisation sollicitée qui portait en l'espèce sur la communication de données à caractère personnel émanant du Centre commun d'affiliation et de perception de sécurité sociale à un institut de sondage qui envisageait d'utiliser les données pour déterminer un échantillon de personnes à interroger comme échantillon représentatif de la population (réutilisation des données). Dans cette affaire-ci, l'aspect scientifique de l'étude prévue n'a pas été jugé suffisamment établi pour justifier l'application de l'article 4 paragraphe (2) de la loi qui permet un traitement des données si nécessaire à des fins scientifiques.

Outre les séances d'informations, workshops, formations et conférences à l'occasion desquels les membres de la Commission nationale ont expliqué les dispositions légales et leurs applications pratiques, il y a lieu de relever en particulier leur participation à un séminaire organisé durant la Présidence luxembourgeoise de l'union européenne par le Ministère de la Fonction publique et de la Réforme administrative dans le cadre de l'EPAN (European Public Administration Network) au sujet de l'interopérabilité des fichiers et de l'échange de données entre administrations.

La Commission nationale a collaboré à une étude confiée au CRP-Gabriel Lippmann et a exposé le point de vue de la protection des données relatif à l'usage d'un identifiant unique des individus dans ce contexte.

Les membres de la Commission nationale ont aussi activement pris part aux travaux des groupes de travail fonctionnant sur le plan européen dans le domaine de la protection des données, y compris ceux relatifs au système d'information Schengen, Europol et des Douanes, où ils ont procédé dans le cadre de l'autorité de contrôle spécifique de l'article 17 à une inspection des services de Police, Douanes et frontières de l'aéroport du Findel.

Lors de la 27e Conférence internationale des commissaires à la protection des données à Montreux (Suisse), qui s'est tenue du 14 au 16 septembre 2005, la session consacrée à "la réglementation des flux transfrontières de données à l'épreuve de la globalisation", eut lieu sous la présidence du représentant luxembourgeois Gérard Lommel, président de la Commission nationale pour la protection des données.

1.3 Activités en 2006

Pour l'année 2006, la Commission nationale avait retenu trois axes prioritaires autour desquels s'agençait son action :

- La poursuite de sa politique d'information du public, des citoyens et des contacts sectoriels ;
- Des efforts pour apporter des solutions ou du moins, des réponses plus concrètes face aux demandes de renseignements et de vérification de la licéité de traitements de données reçues et dans la guidance des acteurs ;
- Une accélération du traitement des demandes d'autorisation.

Sur ce dernier point, il y a lieu de noter que le nombre de dossiers évacués (200) tend à se rapprocher de celui des demandes introduites (295).

Il reste toutefois un volume important de dossiers en cours d'examen (plus de 1300) qui ne sera pas résorbé par les allégements prévus au projet de loi N°5554 portant révision de la loi du 2 août 2002, en particulier par certaines simplifications des formalités administratives obligatoires. 80 % de ces demandes ont pour objet l'autorisation de traitements à des fins de surveillance dont une majorité vise aussi bien celle du personnel que celle des clients, passants et tiers. Viennent ensuite les dossiers concernant des données sensibles et relatives à la santé.

Il s'agit là des traitements de données que le législateur a entendu soumettre au contrôle préalable de l'autorité instituée en vue de surveiller l'application de la loi conformément à l'article 20 § 1er de la directive européenne qui vise ceux comportant des risques particuliers au regard des droits et libertés des personnes concernées.

Certes, la rapidité de l'examen des demandes d'autorisation a pu être sensiblement améliorée au cours de l'année 2006 (et des progrès se feront encore davantage sentir en 2007), toujours est-il que les critères de légitimité et de proportionnalité, de caractère compatible de la finalité de l'utilisation, de la durée et des conditions de conservation des données devront toujours être appréciés « in concreto » en fonction des circonstances particulières de chaque demande, de sorte qu'il sera impossible de recourir à une standardisation outrancière des décisions de la Commission nationale pour la protection des données

Il s'avère ainsi que les effectifs actuels sont toujours insuffisants et devront être renforcés.

Au niveau tant organisationnel que qualitatif, des progrès ont cependant été réalisés, non seulement dans l'analyse des dossiers, mais aussi dans les réponses fournies aux demandes de renseignement (nombreuses, surtout par voie téléphonique : plus de 1900 en 2006) et dans l'information du public et la guidance des responsables de traitements de données.

Le calendrier publié en collaboration avec l'Union Luxembourgeoise des Consommateurs a été diffusé à plus ou moins 50.000 exemplaires et connut un vif succès. Illustré par des caricatures amusantes, il comprend des textes explicatifs qui en font un excellent support de vulgarisation des principes essentiels de la protection des données.

Le site Internet de la Commission nationale a été enrichi de pages thématiques et de nouvelles rubriques et a été mis à jour régulièrement.

Les statistiques des visites (13.000 par mois) démontrent qu'il a atteint un niveau de notoriété respectable et attestent que ce moyen est utilisé comme source d'informations par un public averti de responsables d'entreprises, d'organisations et de juristes spécialisés.

Dès le début de l'année la décision de refus d'autorisation (décembre 2005) du dispositif de contrôle d'accès au moyen de l'authentification des empreintes digitales des abonnés mis en place par le Centre thermal de Mondorf suscitait un vif intérêt de la presse et de l'opinion publique pour la problématique de la collecte et du stockage de données biométriques. Suite à cette décision de refus, le Centre thermal de Mondorf a modifié le système d'authentification consistant à stocker les données biométriques uniquement sur les bracelets-chips détenus par les seuls abonnés. Le système ainsi notifié a été autorisé par la Commission nationale en avril 2006.

La prise de position publiée par la Commission nationale à l'égard du projet de loi N°5356 relative aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle, en octobre 2004, a été elle aussi commentée par des articles de presse au cours du débat parlementaire.

Un autre sujet largement couvert par la presse en 2006 était celui de l'accès des autorités américaines aux données relatives aux transactions financières transitant par le réseau SWIFT. Le manque de transparence sur les limites et les conditions dans lesquelles cet accès a lieu depuis la fin de 2001 a suscité aussi l'inquiétude des députés européens et du groupe européen des commissaires à la protection des données (dit de l'article 29) qui se prononçait publiquement au sujet du non respect des dispositions du droit européen, en demandant des mesures immédiates pour revenir à une situation conforme.

La Commission nationale pour la protection des données a noué un dialogue constructif avec l'ALMUS (Association Luxembourgeoise des Membres et Utilisateurs de SWIFT) et l'ABBL dans ce dossier où ses collègues de la Commission belge de la protection de la vie privée ont la compétence primaire, le siège de SWIFT se trouvant (à la Hulpe) en Belgique. Les banques luxembourgeoises sont intervenues pour améliorer l'information des clients sur les circuits internationaux qu'empruntent les informations relatives à certaines transactions financières internationales.

Un sujet soulevé fréquemment par les responsables d'entreprises (surtout de celles de dimension internationale) est celui des conditions et limites des dispositifs de signalement de dysfonctionnement et d'alerte professionnelle (« whistleblowing ») dans les domaines bancaires de la comptabilité, du contrôle interne des comptes, de l'audit et de la lutte contre la corruption et les données financières. La Commission nationale eut l'occasion à plusieurs reprises (notamment lors d'une conférence réunissant les « compliance officers » de la place financière) de fournir des explications sur la compatibilité avec la loi sur la protection des données dans ce domaine.

Un autre thème qui se retrouvait sous divers aspects dans les travaux de l'année 2006 est celui des données relatives à la santé.

Le passage en revue des infrastructures techniques, pratiques et procédures appliquées au Centre Commun de la Sécurité Sociale et aux fichiers utilisés par l'Union des Caisses de Maladie et les différentes Caisses de Maladie ainsi que d'autres organismes de la sécurité sociale, fut poursuivi avec le soutien des directions des principales entités concernées. Après la validation d'un rapport d'audit établi ensemble avec un expert externe dans lequel furent consignées les recommandations d'amélioration à apporter au cours des années à venir, la Commission nationale délivrait les autorisations respectives requises aux termes des articles 7 et 14 de la loi en examinant de façon critique les questions relatives à la communication des données à d'autres administrations et les mesures de sécurité organisationnelle et technique.

Au niveau du dialogue avec les administrations et organismes publics, il y a lieu de signaler plusieurs chantiers importants de l'exercice écoulé :

- Spécification et introduction du Passeport biométrique (avec le Ministère des Affaires étrangères et le Centre Informatique de l'Etat) ;
- Fichiers des permis de conduire, des immatriculations et échange de données ;
- Carnet radiologique et projet « e-Santé » (Ministère de la Santé) ;
- Projets de recherche scientifique et médicaux (CNER et CRP-Santé) ;

- Simplification administrative et utilisation de l'identifiant unique des personnes pour l'échange et le partage de données entre administrations (CNSAE) ;
- Localisation des numéros d'appel et mise en œuvre de l'article 41 de la loi (ILR)

Outre sa participation aux groupes de travail européens en matière de protection des données (article 29, Case Handling Workshop, Internet Taskforce et Groupe Berlin (secteur des télécoms), la Commission nationale a pris part aux réunions de la Conférence européenne des commissaires à la protection des données, des autorités conjointes, d'Europol, des Douanes et du système d'information Schengen.

Pour la première fois, les autorités de protection des données des Etats membres de l'Union européenne ont lancé en mars 2006 une action coordonnée de contrôle à l'échelle européenne, dans le cadre des activités de leur groupe de travail dit groupe "Article 29". L'objectif de cette action commune consistait à analyser dans quelle mesure et de quelle manière les règles de protection des données personnelles sont respectées par les entreprises privées opérant dans le secteur de l'assurance santé.

Ce secteur a été sélectionné pour deux raisons principales:

- d'une part le traitement de données sensibles est un élément clé des activités concernées;
- d'autre part le non-respect des règles applicables dans ce secteur aurait un impact important sur un grand nombre de personnes dans l'Union européenne

Deux de ses membres composent ensemble avec le délégué du Procureur Général (qui la préside) l'autorité spécifique de contrôle instituée par l'article 17 de la loi pour la surveillance de l'application de la loi par la Police grand-ducale, l'Inspection générale de la Police, l'Administration des Douanes et Accises, dans le domaine de la défense et de la sûreté de l'Etat.

Ses travaux font l'objet d'un rapport spécifique, publié par l'autorité de contrôle de l'article 17.

La Commission nationale pour la protection des données pour sa part a procédé en 2006 à une investigation auprès des services du Ministère des Affaires étrangères et de l'Immigration chargés de la participation au réseau Eurodac.

Ses membres ont présenté des exposés lors d'une douzaine de conférences publiques ou séances d'information sectorielles (IFE, EGCA, Association des gérants d'immeubles) respectivement assuré des formations (INAP, AmCham, CRP-Henri Tudor, LTE Esch-sur-Alzette, Uni Luxembourg, etc.).

La concertation avec les acteurs économiques, les entreprises (petites ou parmi les plus grandes) et professionnels ne fut pas moins intensive.

La Commission nationale eut à examiner les flux des données clients et les règles gouvernant les fichiers à l'accès aux données de quelques entreprises multinationales, notamment parmi celles actives dans le domaine des nouvelles technologies de l'information et des communications qui viennent de s'établir à Luxembourg. Il est apparu nécessaire aux yeux des membres de la Commission nationale de contribuer à l'attractivité du site économique en faisant preuve d'une grande disponibilité et écoute en vue de l'évacuation rapide des formalités obligatoires.

Finalement, elle a continué ses efforts de promotion des modèles de code de conduite sectoriels existant dans d'autres pays ou au niveau européen et d'encourager les entreprises et organisations à désigner un chargé de la protection des données. L'encadrement et la formation continue de ces derniers demandera encore des moyens supplémentaires à l'avenir, surtout si la flexibilisation de leur statut (prévue dans le projet de loi) contribuera à populariser davantage cette institution comme nous l'observons actuellement en France (après l'Allemagne et les Pays-Bas).

1.4 Développements informatiques

La Commission nationale a fait des efforts considérables pour développer et améliorer son environnement informatique tant au niveau de son réseau local qu'au niveau des systèmes de gestion de ses affaires.

1.4.1 Nouveau formulaire de notification

La Commission nationale avait retenu pour l'élaboration des formulaires de notification et notification simplifiée la solution basée sur le format PDF d'Adobe Acrobat. Afin de permettre aux utilisateurs finaux une gestion conviviale de leurs notifications et notifications simplifiées, la Commission nationale a également développé une application intégrant les formulaires et permettant la sauvegarde et l'envoi via Internet des données saisies. Les désavantages de cette solution étaient néanmoins la limitation de l'utilisation de l'application à un environnement Microsoft ainsi qu'à la version 5 d'Adobe.

Ainsi, la Commission nationale a effectué une étude portant sur la viabilité d'une solution pour l'édition, la sauvegarde et l'envoi via Internet sécurisé des formulaires de notification et pour fonctionner sous les différents systèmes d'exploitation tels que Mac OS X, Microsoft Windows, Linux.

Afin de pouvoir prendre la bonne approche pour l'avenir, la Commission nationale a fait l'inventaire des différents formulaires de notifications dans les pays d'Europe et a comparé les différentes options. Finalement, la Commission nationale a retenu la solution d'Adobe (formulaire PDF basé sur Reader Extension) qui permet notamment la sauvegarde des données saisies dans le formulaire et l'envoi sécurisé direct des données via Internet.

Dans un souci d'adaptation à l'évolution technologique, la Commission nationale a décidé de revoir différents aspects du formulaire (catégories de données qui sont traitées, durée de conservation, etc) pour ensuite développer un nouveau formulaire regroupant tous les types de déclaration n'étant pas soumis à autorisation préalable, c'est-à-dire la notification et la modification d'une notification ordinaire et simplifiée. Une aide directe a été intégrée dans le nouveau formulaire qui peut en outre être rempli en langue française et allemande.

1.4.2 Gestion informatique interne des déclarations (notifications et demandes d'autorisation)

La Commission nationale a mis en œuvre une application informatique centralisée pour gérer et suivre les dossiers ainsi que pour assurer la publicité des traitements en vertu de l'article 15 de la loi (registre public). De par son caractère centralisé, l'application permet le travail en groupe et améliore la coordination entre ses différents services.

Le workflow ainsi élaboré assure :

- la saisie des données dans le formulaire, la sauvegarde et l'envoi sécurisé via Internet;
- l'importation des données dans l'application de gestion des déclarations;
- la gestion des déclarations (enregistrement, contrôle, suivi, rapports, statistiques, etc) ;
- le transfert vers le registre public.

1.4.3 Registre public des traitements déclarés à la Commission nationale

En vertu de l'article 15 de la loi du 2 août 2002, la Commission nationale doit assurer la publicité des traitements lui déclarés (notifications effectuées, traitements autorisés). Pour ce faire, elle a mis en œuvre une interface Internet permettant d'effectuer un certain nombre d'affichages et de recherches. Le registre s'appuie sur une base de données relationnelle exportée à partir de l'application de gestion interne.

1.4.4 Site Internet de la Commission nationale migré et révisé

Dans le cadre du programme « eLëtzebuerg » et de la charte informatique prévoyant un lay-out commun à tous les sites Internet des administrations de l'Etat, la Commission nationale a effectué une migration sur les serveurs du CIE. De même, dans un souci de mieux tenir compte des besoins des utilisateurs, elle a procédé à une révision profonde du contenu et de la structure du site.

1.4.5 Chargés de la protection des données

La Commission nationale a élaboré une procédure permettant aux chargés de la protection des données d'établir leur registre des traitements surveillés et de le continuer à la Commission nationale, afin de pouvoir le publier au registre public des traitements.

1.4.6 Gestion interne du flux des documents

La Commission Nationale a élaboré divers applications internes facilitant la gestion des flux des documents et la confection des statistiques.

1.5 Avis et décisions publiés par la Commission nationale

(reproduits dans l'annexe 2 du présent rapport)

- Délibération n° 3/2004 du 20 février 2004 portant avis de la Commission nationale pour la protection des données au sujet du projet de la loi n° 5181 portant transposition de la directive 2002/58/CE « vie privée et communications électroniques » et modification de la loi du 2 août 2002.

La Commission nationale pour la protection des données a publié son avis relatif à ce projet de loi le 20 février 2004. La loi a été finalement adoptée par le Parlement le 30 mai 2005 et est entrée en vigueur le 1er juillet 2005.

- Délibération n° 4/2004 du 20 février 2004 portant avis de la Commission nationale pour la protection des données au sujet de l'avant-projet de règlement grand-ducal fixant les modalités ayant trait aux missions du chargé de la protection des données.
- Délibération n° 74/2004 du 13 septembre 2004 de la Commission nationale pour la protection des données concernant la loi du 6 juillet 2004 modifiant la loi du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques.
- Délibération nº76/2004 du 17 septembre 2004 de la Commission nationale pour la protection des données relative au sujet de la demande du Fonds de garantie automobile à la direction générale de la police grand-ducale.
- Délibération n°78/2004 du 8 octobre 2004 de la Commission nationale pour la protection des données concernant le projet de loi n° 5356 relatif aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle.
- Délibération n°84/2004 du 15 novembre 2004. Avis de la Commission nationale pour la protection des données concernant le projet de règlement grand-ducal déterminant les services de communications électroniques et les services postaux ainsi que la nature, le format et les modalités de mise à disposition des données dans le cadre de l'article 41 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.
- Communiqué de presse du 18 janvier 2005 concernant la licéité des tests de paternité qui a reçu une large couverture dans les médias.

- Délibération n°66/2005 du 4 mai 2005 de la Commission nationale pour la protection des données concernant l'avant-projet de loi relatif à l'accès des officiers de police judiciaire à certains traitements de données à caractère personnel des personnes morales de droit public.
- Délibération n°73/2005 du 1er juillet 2005 de la Commission nationale pour la protection des données relative à la demande d'autorisation préalable en matière surveillance du courrier électronique, de l'Internet et du réseau informatique introduite par Odyssey Asset Management Systems S.A. Luxembourg.
- Délibération n°84/2005 du 11 novembre 2005 de la Commission nationale pour la protection des données concernant l'avant-projet de loi sur le contrôle des voyageurs dans les établissements d'hébergement et au projet de règlement grand-ducal relatif au modèle des fiches à tenir par les tenanciers d'établissements d'hébergement introduite par le Ministère des Classes Moyennes, du Tourisme et du Logement (Monsieur le Ministre Fernand BODEN).
- Délibération n°85/2005 du 5 décembre 2005 de la Commission nationale pour la protection des données concernant le projet de loi portant modification de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel introduite par Monsieur le Ministre délégué aux Communications Jean-Louis SCHILTZ.
- Délibération n°89/2005 du 21 décembre 2005 de la Commission nationale pour la protection des données relative à la demande d'autorisation préalable introduite par l'établissement public Domaine Thermal de Mondorf en matière de traitement à des fins de surveillance contenant des données biométriques.
- Délibération n°33/2006 du 12 avril 2006 de la Commission nationale pour la protection des données relative à la demande d'autorisation préalable en matière de traitement à des fins de surveillance contenant des données biométriques introduite par le Domaine Thermal de Mondorf.
- Délibération n°136/2006 du 22 décembre 2006 Avis de la Commission nationale pour la protection des données relatif à la numérisation d'actes de l'état civil de la commune de Lintgen par un prestataire de services privé.

1.6 Participation aux travaux sur le plan international

Les membres effectifs étaient régulièrement en contact avec leurs homologues allemands, belges et français et d'autres Etats membres de l'Union Européenne. Leurs conseils, tout comme les discussions menées au niveau des groupes de travail européens, ont permis aux membres de la Commission nationale de perfectionner leurs connaissances en la matière et de profiter de l'expérience des autres autorités de contrôle fonctionnant au niveau national.

Le groupe de l'article 29 joue à ce titre un rôle de coordination central et les documents de réflexions et prises de position qui en émanent représentent une documentation essentielle pour nourrir les réflexions de notre Commission nationale.

Aussi, la participation à ses séances et aux groupes de travail sporadiques qui en émanent (Complaints Workshop, Internet Task Force etc.) est jugée indispensable pour la formation continue, l'échange d'expériences et la remise en question des trois membres effectifs avant même de prendre en considération les nécessités d'y représenter convenablement le Grand-Duché.

Il en est de même de la Conférence Européenne (annuelle) des autorités de contrôle européennes en matière de protection des données qui eût lieu à Rotterdam (Pays-Bas) en avril 2004, à Cracovie (Pologne) en avril 2005 et à Budapest (Hongrie) en avril 2006, des séminaires ponctuels (gestion des plaintes, combat du spam et risques nouveaux engendrés par les nouvelles technologies de l'information et de la communication) et des réunions des autorités de contrôle conjointes instaurées auprès d'Europol respectivement chargées de surveiller le fonctionnement du système d'information Schengen auxquelles l'un ou l'autre des membres de la CNPD a participé chaque fois que cela s'imposait.

Certaines questions abordées lors de ces réunions internationales évoquaient d'ailleurs des sujets d'actualité brûlante au Grand-Duché, comme ceux des données génétiques, de l'usage de données biométriques à des fins d'authentification et de sécurité, de la surveillance exercée par l'employeur dans le contexte du travail et de la vidéosurveillance, des limites de la réutilisation de données publiques par des tiers, des traitement de données à des fins de marketing direct, de l'articulation entre les législations concernant la protection des données et le combat du blanchiment d'argent et du financement du terrorisme, etc.

Un document de travail adopté par le Groupe de l'article 29 le 3 juin 2003 encourage les autorités nationales de contrôle à innover et à retenir des « règles d'entreprises contraignantes » comme garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes pour autoriser le transfert de données à caractère personnel par une entité d'un groupe multinational établie sur leur territoire vers des pays tiers n'assurant pas un niveau de protection adéquat. Un tel cas de figure pourrait rapidement se présenter au Grand-Duché parmi les entreprises y opérant une filiale ou succursale et dont les maisons-mères sont situées aux Etats-Unis ou dans d'autres pays hors Union européenne.

Il appartiendra à la Commission nationale de relever le défi et de jouer pleinement son rôle dans des situations concrètes, le cas échéant délicates, et non dépourvues d'incidence sur la compétitivité du site économique luxembourgeois.

2. Bilan et perspectives

2.1 Objectifs prioritaires et mise en œuvre de la démarche stratégique adoptée par la Commission nationale pour la protection des données

Aux deux tiers de la durée du premier mandat de la Commission nationale, ses membres se sentent à la fois confirmés dans les choix retenus au niveau de sa démarche tout en ne sous-estimant pas les difficultés rencontrées. Rappelons que dans son précédent rapport d'activité elle avait défini comme suit son approche pour l'exécution de ses missions :

« ***Approche et objectifs prioritaires de la CNPD***

Les axes stratégiques suivants ont été dégagés dès les premiers mois d'activité de la Commission nationale :

- Réveiller les consciences et sensibiliser
- Devenir force de proposition et propager des standards de bonne pratique
- Stimuler la vigilance des citoyens
- Encourager l'autodiscipline des acteurs et favoriser la co-régulation

Les moyens d'une telle politique qui se veut délibérément respectueuse des impératifs du bon fonctionnement de l'administration publique et des contraintes et besoins du monde des affaires et des autres professionnels, seront par prédilection l'information, la sensibilisation et la responsabilisation.

La Commission nationale est consciente qu'elle doit faire preuve d'ouverture au dialogue, de pédagogie, de pondération et de disponibilité et devra éviter tout écueil bureaucratique stérile. Au contraire il s'agit de faire preuve de force de persuasion et de démontrer en pratique la valeur ajoutée apportée au niveau du climat de confiance par une saine politique de protection de la vie privée et des données personnelles. Etre pôle de compétence, source de guidance, autorité de contrôle et de réception des plaintes devra aller de pair avec une appréciation réaliste et une communication habile en vue de la mise en balance équitable des intérêts bien compris aussi bien des responsables du traitement que des citoyens administrés, consommateurs, utilisateurs et salariés.

Il y a lieu toutefois de ne pas sous-estimer l'évolution nécessaire des mentalités et les moyens nécessaires pour pouvoir assurer dans de bonnes conditions les missions confiées par la loi à la Commission nationale en application des règles de la directive européenne 95/46/CE et de la Convention 108 du Conseil de l'Europe.

Pour un déploiement progressif de son action les membres de la Commission nationale estiment avoir besoin des 6 années de leur premier mandat.

Une road map sur six ans avec des accents prioritaires

Années ***1 - 2*** : *Mise en place des services, formation et organisation interne, fonctionnement des procédures et flux administratifs, contacts et guidances des responsables de traitement, avis au gouvernement*

3 - 4 : *Campagne d'information du public, analyse de cas exemplaires, recommandations thématiques, dialogue constructif avec des organisations sectorielles représentatives, stimuler le débat public et la prise de conscience des citoyens et acteurs professionnels*

5 - 6 : *Promouvoir une culture de protection des données, favoriser l'autocontrôle par les personnes concernées et l'autodiscipline des acteurs professionnels, encourager l'élaboration de codes de conduite sectoriels, de chartes et politiques internes (de groupes d'entreprises et de l'administration publique p.ex.) »*

2.2 Expliquer la loi, sensibiliser les citoyens, promouvoir les bonnes pratiques

L'accent mis sur l'information du public et la guidance des acteurs, en parallèle aux missions de contrôle (a priori et a posteriori) et la publication de recommandations à l'adresse des pouvoirs publics, se retrouve mis en évidence dans une déclaration solennelle, appelée encore initiative de Londres (2-3 novembre 2006), proclamée lors de la 28ème Conférence international des Commissaires à la Protection des Données et de la Vie Privée, comme priorité à mettre au tout premier plan dans l'action quotidienne des autorités de contrôle mises en place en application de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995.

Cette conclusion a été dégagée suite au constat que la protection des données personnelles des individus doit faire face actuellement à un triple défi :

a) celui de l'accélération du développement technologique et de la globalisation générant de nouveaux risques,

b) celui des développements de législations anti-terroristes et destinées à renforcer la sécurité publique, engendrant le piège de la remise en cause progressive des libertés citoyennes,

c) celui de la réputation de la protection des données souvent mise à mal par une perception négative d'exagération et d'irréalisme, de complexité excessive et de contrainte administrative et, à l'inverse, d'efficacité défaillante du cadre légal et des autorités de contrôle lorsque les attentes sont trop grandes.

Pour rendre la protection des données plus effective, la conférence internationale préconise une nouvelle stratégie de communication des autorités de contrôle, misant aussi sur le développement de la capacité d'expertise, de prospective et d'intervention dans le domaine technologique, sur une démarche positive de dialogue orienté sur la proposition de solutions et la promotion de modèles de bonne pratique.

2.3 La simplification des obligations formelles imposées aux responsables des traitements de données et une meilleure harmonisation de l'application de la directive à travers l'Union européenne.

Dans son premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE) COM 265 du 15 mai 2003, la Commission européenne recommandait au Parlement européen et au Conseil de ne pas apporter de modifications au texte de la directive mais d'œuvrer par d'autres voies à une simplification et une harmonisation de sa mise en pratique dans les différents Etats membres.

Elle estime que ces règles, assurant un niveau de protection élevé aux citoyens, ont aboli ou évité d'éventuels obstacles à la libre circulation des données au sein du marché intérieur et fondent un climat de confiance favorable au développement du commerce électronique et du recours croissant aux technologies de l'information et des communications par l'administration publique qui se modernise.

La Commission européenne fait aussi expressément appel aux Etats membres de faire largement usage des possibilités d'exemption de l'obligation de notification offertes par la directive et de simplifier les formalités administratives et, en même temps, d'aligner leurs lois nationales autant que possible sur le texte de la directive en vue d'éviter des disparités nationales inutiles.

Le projet de loi N°5554 promet de traduire cette volonté dans la loi luxembourgeoise. Rappelons que le programme gouvernemental publié en août 2004 retenait qu'il serait « *procédé rapidement à une révision de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel avec comme objectif primaire de clarifier et de simplifier les procédures de façon à éliminer certains obstacles purement administratifs sans plus-value pour la protection de la vie privée et les libertés individuelles* ».

Dans sa communication du 7 mars 2007 relative au suivi du programme de travail, la Commission européenne souligne par ailleurs le rôle du groupe de travail dit « de l'article 29 » dans le développement d'une interprétation uniforme et de l'adaptation des pratiques des autorités nationales, tout en soulignant que l'adoption du traité constitutionnel, qui intègre la Charte des droits fondamentaux, représenterait une avancée, non seulement dans la reconnaissance du droit universel des individus à la protection des données personnelles, mais aurait une base juridique spécifique et autonome permettant à l'Union de légiférer en la matière au-delà de la limitation actuelle en dépassant l'actuelle division en piliers.

Le projet de décision-cadre visant à harmoniser les règles relatives à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, discuté actuellement au niveau du Conseil revêt une importance cruciale pour l'établissement de standards ambitieux de protection de la vie privée dans les domaines du 3ème pilier (à côté des règles existantes : Europol, Eurojust, Schengen, Prüm, …)

Sur le plan national, la simplification des procédures devrait permettre également de désengorger la Commission nationale au niveau de ses tâches administratives pour lui permettre de mieux se consacrer sur ses autres missions :

- Le traitement des plaintes, la vérification de licéité et les investigations ;
- La sensibilisation du public et la stimulation de la vigilance des citoyens ;
- La guidance des acteurs et la promotion de l'autorégulation.

Compte tenu du nombre de demandes d'autorisation préalable restant à évacuer, cela n'ira pas sans renforcement concomitant des effectifs en personnel.

Au cours des discussions au sein du Comité national pour la simplification administrative dans l'intérêt des entreprises (CNSAE), mis en place par le gouvernement sous l'auspice conjoint des Ministres des Classes Moyennes et de l'Economie, la simplification et modernisation de la loi du 2 août 2002 relative à la protection des données à caractère personnel fut reconnue comme un élément important pour le succès des efforts gouvernementaux de simplification administrative en faveur des entreprises. Voilà aussi une raison pour lui donner les moyens de corriger au plus vite les retards regrettables dans le traitement des formalités administratives et de simplifier celles-ci pour la rendre plus disponible à l'égard des demandes des citoyens.

Un préalable identifié dans les conclusions tirées des travaux de ce Comité consiste dans l'adaptation du cadre légal en vue de faciliter l'interconnexion des données traitées dans des fichiers de différentes administrations notamment au moyen d'un identifiant unique des individus et des citoyens.

La Commission nationale n'a cependant pas manqué de souligner que ce phénomène devait rester limité et strictement encadré par les conditions de la loi sur la protection des données et comporter des garanties appropriées pour le respect de la vie privée (en particulier l'article 16 qui exige l'autorisation préalable).

Les membres de la Commission nationale n'ont pas exclu de pouvoir se prononcer favorablement à un assouplissement du paragraphe 3 dudit article, en particulier par le remplacement de l'exigence que les utilisations rendues possibles par l'interconnexion soient compatibles (entre elles) plutôt que limitées aux seules finalités identiques (comme actuellement).

Le CNSAE a présenté au début 2006 le résultat d'une enquête menée auprès de 500 entreprises représentatives du pays.

Il en résulte que 78% des réponses admettent l'utilité des obligations administratives imposées aux entreprises (13 % ne l'admettent pas et 8 % ne savent pas), seulement 73 % ne trouvent pas la charge imposée aux entreprises trop lourde.

Seul 2% se plaignent de leurs relations avec l'administration compétente (l'un des meilleurs scores de l'étude), mais 20 % répondent qu'ils ne peuvent pas encore les juger.

Ces chiffres sont en ligne avec l'enquête présentée début 2004 par la Commission européenne où un quart des entreprises admettaient qu'il leur faudrait encore du temps pour s'adapter aux nouvelles exigences légales qu'un tiers des responsables interrogés avouaient ne pas encore connaître suffisamment bien.

Il en résulte que les efforts que la Commission nationale consacre à la guidance des entreprises et organisations, et qu'elle souhaite élargir à l'avenir, sont nécessaires.

Il en va de même des ressources investies dans l'information du public et la sensibilisation des citoyens alors que la Commission européenne y voit la plus grande faiblesse (la faible connaissance des règles applicables) dans la mise en œuvre de la directive.

Les membres de la Commission nationale s'accordent toutefois à noter un progrès sensible dans la visibilité de son action auprès du public en général et de la prise en compte du cadre légal par les responsables des traitements de données et s'inscrivent donc en faux face à l'appréciation exprimée de façon isolée dans la presse quotidienne que la loi serait un échec.

III Ressources et Structures

1 Finances

1.1 Rapport de gestion 2004

Il est à noter que la dotation allouée à l'établissement public pour 2004 par l'Etat tenait compte pour la première fois d'un budget complet établi par la Commission nationale elle-même et approuvé par le gouvernement en application de l'article 37 paragraphe (3) de la loi. Les dépenses et recettes effectives sont donc très largement en ligne avec les prévisions.

- Dépenses de fonctionnement

Le cadre du personnel comprend outre les trois membres effectifs de la Commission nationale deux postes de fonctionnaires de la carrière moyenne (rédacteur) et est complété par un employé public à durée indéterminée assurant le secrétariat. Le recours à des renforts temporaires extérieurs s'est donc avéré indispensable afin d'être en mesure de réceptionner et de commencer à traiter les quelques 7200 dossiers, dont 3500 notifications reçues depuis l'entrée en vigueur de la loi.

Les auxiliaires temporaires que l'établissement public s'est vu affecter par l'Administration de l'Emploi au cours de l'année 2004 (une douzaine) ont eux aussi collaboré activement au démarrage et au rodage des structures administratives de la Commission nationale, bien qu'avec une durée moyenne de contrat d'à peine 3 mois, ces auxiliaires n'assurent pas une continuité suffisante permettant de confier aux demandeurs d'emploi en question – aussi qualifiés et motivés soient-ils - des tâches complexes et essentielles dans l'activité de la Commission.

La Commission nationale a dû recourir également à des prestations de services informatiques et à des consultations juridiques extérieures à défaut de disposer des ressources nécessaires en interne, bien qu'il eut été sans doute préférable pour la continuité du service, d'acquérir et de conserver les compétences afférentes au sein de l'établissement public.

La mise en place de ses services explique également les investissements auxquels la Commission nationale a dû procéder en 2004, à savoir l'acquisition des meubles et équipements de bureau, des ordinateurs nécessaires à son réseau informatique interne ainsi qu'au développement et à la mise en service de l'application informatique spécifique dédiée à l'établissement du registre public des traitements prévu à l'article 15 de la loi et au suivi des dossiers de notifications et demandes d'autorisation préalables ainsi qu'à l'optimisation des procédures administratives.

Le formulaire servant à la notification des traitements de données a été considérablement amélioré et permet désormais aux déclarants une meilleure convivialité dans l'utilisation et simplifie la gestion de leurs déclarations.

Ensemble avec l'accroissement des rémunérations et des frais du personnel et de frais de personnel, les frais d'entretien des locaux, les fournitures de bureau, les frais de port et de télécommunications et autres charges générales d'exploitation ont connu une progression linéaire suivant l'augmentation du nombre de collaborateurs en activité.

Il est à noter par ailleurs que la Commission nationale n'a pas encore eu à supporter en 2004 de loyers et charges locatives, les locaux où sont installés ses bureaux lui étant mis à disposition par l'Etat conformément à l'article 37 alinéa 1er de la loi du 2 août 2002 sur la protection des données.

Comme prévu, les dépenses de communication ont connu une augmentation significative du fait de l'élargissement du travail d'information au grand public (édition et diffusion d'une brochure en collaboration avec le Service Information et Presse du gouvernement, affiches et annonces dans la presse).

Les frais de déplacement et de séjour à l'étranger sont relatifs à la participation des membres effectifs de la Commission nationale aux différentes réunions, séances de travail et conférences organisées sur le plan européen dans le domaine de la protection des données où le Luxembourg se doit d'être représenté.

Les amortissements comptabilisés atteignent un montant total de 42.517,- € et n'expliquent pas les investissements initiaux liés à la mise en place initiale des infrastructures nécessaires au fonctionnement de la Commission nationale.

Les frais de fonctionnement encourus par l'établissement public au cours de l'exercice 2004 s'élèvent à un total de 979.534,56 €.

- Recettes

Le montant des redevances perçues en application des articles 37 paragraphe (4) et 13 paragraphe (4) de la loi s'élève à 70.688,- €. La diminution du nombre de notifications effectuées par les responsables de traitement de données explique la baisse du montant total de redevances afférentes perçues. En outre des produits financiers ont pu être enregistrés à hauteur de 8.044,- €.

- Résultat d'exploitation

Compte tenu de la dotation annuelle de 900.000.- € dont la Commission nationale a bénéficié en 2004 de la part de l'Etat en application de l'article 37 paragraphe (4) de la loi, le résultat d'exploitation de l'établissement public s'établit à 5.604.28,- € au 31 décembre 2004, montant qui sera reporté à nouveau sur l'exercice suivant.

1.2 Rapport de gestion 2005

Il est à noter que la Commission nationale a connu une modification dans sa composition par le départ d'un membre effectif en milieu d'année, Monsieur Edouard Delosch ayant été remplacé le 18 octobre 2005 par Monsieur Thierry Lallemang qui occupait jusque là le poste de juriste au service juridique et de documentation.

- Dépenses de fonctionnement

Le cadre du personnel comprend outre les trois membres effectifs de la Commission nationale deux postes de fonctionnaires de la carrière moyenne (rédacteur) et est complété par un employé public à durée indéterminée assurant le secrétariat et par un juriste à durée déterminée affecté au service juridique.

Les deux fonctionnaires ont terminé avec succès leur période de stage et ont été titularisés comme rédacteur à l'issue de l'examen afférent en avril 2005.

Les vacances temporaires de postes au niveau des employés de l'Etat (juriste, secrétaire) se sont traduites par des économies sur le plan des rémunérations du personnel permanent et des dépenses additionnelles au niveau du personnel de remplacement respectivement de prestations de services de tiers.

Les auxiliaires temporaires (11 au total) que l'établissement public s'est vu affecter par l'Administration de l'Emploi au cours de l'année 2005 ont eux aussi collaboré activement aux travaux administratifs de la Commission nationale.

La Commission nationale a dû recourir en outre à des prestations de services informatiques et à des consultations juridiques extérieures à défaut de disposer en interne des ressources nécessaires, bien qu'il eut été sans doute préférable pour la continuité du service, d'acquérir et de conserver les compétences afférentes au sein de l'établissement public.

La Commission nationale a procédé en 2005 à des investissements relatifs au développement et à la mise en service de l'application informatique spécifique dédiée à l'établissement du registre public des traitements prévu à l'article 15 de la loi et au suivi des dossiers de notifications et demandes d'autorisation préalables ainsi qu'à l'optimisation des procédures administratives. L'essentiel de l'effort financier afférent reposait cependant sur l'exercice 2004.

Le formulaire servant à la notification des traitements de données a été considérablement amélioré et permet désormais aux déclarants une meilleure convivialité dans l'utilisation et simplifie la gestion de leurs déclarations intégrant les versions allemande et française, la notification ordinaire et simplifiée, les lexiques et le guide d'utilisation.

Afin de contribuer à l'amélioration du niveau de sécurité appliqué aux traitements de données à caractère personnel dans l'activité des organismes de la Sécurité Sociale, la Commission Nationale a procédé à un audit de la sécurité avec l'assistance d'un expert externe. Cette analyse se situe dans le cadre de l'examen des demandes d'autorisation qui lui ont été soumises conformément à l'article 14 de la loi et dans l'examen desquelles l'appréciation du niveau approprié des mesures de sécurité organisationnelles et techniques représente un volet important, en particulier au regard des données sensibles traitées par lesdits organismes de sécurité sociale dans leur activité quotidienne.

Les frais d'entretien des locaux, les fournitures de bureau, les frais de port et de télécommunications et autres charges générales d'exploitation ont connu une progression linéaire suivant l'augmentation du nombre de collaborateurs en activité.

Il est à noter par ailleurs que la Commission nationale n'a pas encore eu à supporter en 2005 de loyers et charges locatives, les locaux où sont installés ses bureaux lui étant mis à disposition par l'Etat conformément à l'article 37 alinéa 1er de la loi du 2 août 2002 relative à la protection des données à l'égard du traitement des données à caractère personnel (-96.600€).

Comme prévu au budget, les dépenses de publication et d'information du public ont connu une augmentation significative (+17.819,67€) du fait de l'élargissement de communication au grand public (notamment pour l'élaboration et la diffusion du calendrier 2006 coédité avec l'ULC).

Les frais de déplacement et de séjour à l'étranger sont relatifs à la participation des membres effectifs de la Commission nationale aux différentes réunions, séances de travail et conférences organisées sur le plan européen dans le domaine de la protection des données où le Luxembourg se doit d'être représenté.

Les amortissements comptabilisés atteignent un montant total de 55.066,60€ et n'expliquent pas les investissements initiaux liés à la mise en place initiale des infrastructures nécessaires au fonctionnement de la Commission nationale.

Le total des frais de fonctionnement encourus par l'établissement public au cours de l'exercice 2005 s'élève à 963.014,18€.

- Recettes

Le montant des redevances perçues en application des articles 37 paragraphe (4) et 13 paragraphe (4) de la loi s'élève à 84.465,30€. La diminution du nombre de notifications effectuées par les responsables de traitement de données explique la baisse du montant total de redevances afférentes perçues. En outre des produits financiers ont pu être enregistrés à hauteur de 8.797,60€.

- Résultat d'exploitation

Compte tenu de la dotation annuelle de 978.0000€ dont la Commission nationale a bénéficié en 2005 de la part de l'Etat en application de l'article 37 paragraphe (4) de la loi, le résultat d'exploitation de l'établissement public s'établit à 108.248,72€ au 31 décembre 2005.

Compte tenu que la Commission nationale n'a pas encore eu à supporter en 2005 de loyers et charges locatives, le montant de 96.600€ initialement prévu au budget des dépenses doit être considéré perçu en trop sur la dotation de l'année 2005 et sera imputé sur la dotation prévue au budget de l'Etat de l'année 2006. Le solde de 11.648,72€ est reporté à nouveau sur l'exercice suivant.

1.3 Rapport de gestion 2006

L'activité de la Commission nationale au cours de l'année 2006 a été marquée par

- l'accompagnement du projet de révision de la loi
- le traitement d'un grand nombre de formalités préalables à la mise en œuvre accomplies par les responsables en application du chapitre III de la loi
- les efforts déployés pour en optimiser la procédure et la prise en charge
- les actions menées en vue de l'information du public et de la guidance des responsables de traitements
- la maintenance et les mises à jour de notre site Internet www.cnpd.lu (hébergé auprès du CIE)
- le développement d'une version allégée en langue anglaise et portugaise de notre site Internet www.cnpd.lu
- les investigations menées en vue de vérifier le respect des obligations légales par les acteurs publics et privés (Centre thermal Mondorf, assurances complémentaires maladie, sécurité sociale)
- la poursuite de sa campagne d'information du public notamment à travers diverses séances d'information et la préparation de la première journée européenne de la protection des données.

- Dépenses de fonctionnement

Les effectifs en personnel de la Commission nationale se composaient en 2006 outre des trois membres effectifs, de deux fonctionnaires de la carrière moyenne (rédacteur), de deux employés à durée indéterminée assurant le secrétariat et d'un employé juriste à durée déterminée affecté au service juridique et de la documentation. Le deuxième poste d'employé de l'Etat (juriste) étant malheureusement resté vacant durant l'année entière, cela s'est traduit par des économies sur le plan des rémunérations du personnel permanent.

Les auxiliaires temporaires que l'établissement public s'est vu affecté par l'Administration de l'Emploi au cours de l'année 2006 (une demi-douzaine) ont eux aussi collaboré activement aux travaux administratifs de la Commission nationale.

Celle-ci a dû recourir en outre à des prestations de services informatiques et à des consultations juridiques extérieures à défaut de disposer en interne des ressources nécessaires, bien qu'il eut été sans doute préférable pour la continuité du service, d'acquérir et de conserver les compétences afférentes au sein de l'établissement public.

Afin de contribuer à l'amélioration du niveau de sécurité appliqué aux traitements de données à caractère personnel, la Commission Nationale :

- a procédé à un audit de la sécurité avec l'assistance d'un expert externe dans l'activité des organismes de la Sécurité Sociale. Cet audit se situe dans le cadre de l'examen des demandes d'autorisation qui lui ont été soumises conformément à l'article 14 de la loi et dans l'examen desquelles l'appréciation du niveau approprié des mesures de sécurité organisationnelles et techniques représente un volet important, en particulier au regard des données sensibles traitées par lesdits organismes de sécurité sociale dans leur activité quotidienne.
- a procédé à l'analyse et la vérification du fonctionnement d'un dispositif de contrôle d'accès basé sur la reconnaissance des empreintes digitales à Mondorf. L'investigation en question a nécessité le recours à un expert en raison de la complexité technique d'un traitement de données personnelles biométriques.

Les frais d'entretien des locaux, les fournitures de bureau, frais de port et de télécommunications et autres charges générales d'exploitation ont connu une progression linéaire suivant l'augmentation du nombre de collaborateurs en activité.

Il est à noter par ailleurs que la Commission nationale a eu pour la première fois à supporter en 2006 des frais de loyers et de charges locatives (81.055,44€).

Comme prévu au budget, les dépenses de communication s'élèvent à 44.600,34€ compte tenu de la préparation de la première journée européenne de la protection des données.

Les frais de déplacement et de séjour à l'étranger sont relatifs à la participation des membres effectifs de la Commission nationale aux différentes réunions, séances de travail et conférences organisées sur le plan européen dans le domaine de la protection des données où le Luxembourg se doit d'être représenté.

Les amortissements comptabilisés atteignent un montant total de 39.865,96€.

Le total des frais de fonctionnement encourus par l'établissement public au cours de l'exercice 2006 s'élève à 1.045.902,51€.

- Investissements

Au cours de l'exercice 2006 les dépenses d'investissement effectuées restent à un niveau très modeste. Ces dépenses ne resteront pas pour autant forcément aussi faible au cours des exercices à venir, compte tenu des besoins qui se présenteront.

- Recettes

Le montant des redevances perçues en application des articles 37 paragraphe (4) et 13 paragraphe (4) de la loi s'élève à 61.945€. Il est resté sensiblement en retrait par rapport aux prévisions en raison de la diminution du nombre de notifications reçues par les responsables de traitement de données. En outre des produits financiers ont pu être enregistrés à hauteur de 13.529,66€.

- Résultat d'exploitation

Compte tenu de la dotation annuelle de 1.028.100€ dont la Commission nationale a bénéficié en 2006 de la part de l'Etat en application de l'article 37 paragraphe (4) de la loi, le résultat d'exploitation de l'établissement public s'établit à +57.672.15€ au 31 décembre 2006 qui sera reporté à nouveau sur l'exercice suivant.

2. Personnel et services mis en place

Avec le concours de ses membres suppléants, la Commission nationale a élaboré son règlement intérieur (adopté le 29 novembre 2002) et le schéma de notification (adopté le 26 février 2003). Les avis prévus à l'article 43 paragraphe 1er de la loi ont été publiés dans les quotidiens le 7 mars 2003 et au Mémorial B Nº22 du 11 avril 2003.

Conformément à son règlement intérieur, les services suivants ont été mis en place depuis 2003 :

- Service juridique et de documentation
- Service informatique et de la logistique
- Tenue du registre public et prise en charge administrative des notifications, demandes d'autorisation et requêtes diverses
- Administration générale et finances
- Service presse et communication

Membres effectifs :	Gérard LOMMEL, président (juriste issu du secteur privé)
Depuis le 18/10/2005	Thierry LALLEMANG, (juriste issu du secteur public)
	Pierre WEIMERSKIRCH, (informaticien issu du secteur public)
Jusqu'au 3/07/2005	Edouard DELOSCH, (juriste issu du secteur public)
Membres suppléants :	Véronique WAGNER, Josiane PAULY (juristes) et François THILL (informaticien)

Service juridique et de documentation

Jusqu'au 18/10/2005	Thierry LALLEMANG, (juriste issu du secteur public)
Depuis le 1er/05/2006	Georges WEILAND, (juriste issu du secteur privé)
Poste en recrutement	juriste, employé de l'Etat à durée déterminée (Service juridique et de documentation)
CAT	assistant service juridique et de documentation

Tenue du registre public et prise en charge administrative des notifications, demandes d'autorisation et requêtes diverses

Monsieur Marc MOSTERT	rédacteur
Monsieur Thomas FRERES	rédacteur
CAT	assistant administratif

Service informatique et de la logistique

CAT	informaticien (Service informatique et de logistique)

Administration générale et finances

Monsieur Jacques BECKER	assistant de direction, employé de l'Etat (Administration générale et finances)
Madame Tania RISCH	employée de l'Etat

Service presse et communication

CAT	assistant service presse et communication

Le début de l'été 2005 a été marqué par le départ de M. Edouard Delosch en tant que membre effectif de la Commission nationale. Il a été remplacé en cette fonction par M. Thierry Lallemang, juriste, qui a été nommé comme nouveau membre sur proposition du Gouvernement en conseil. En présence du Ministre délégué aux Communications M. Jean-Louis Schiltz, M. Lallemang a prêté serment le 18 octobre dans les locaux du Service Médias et Communications du Ministère de l'Etat.

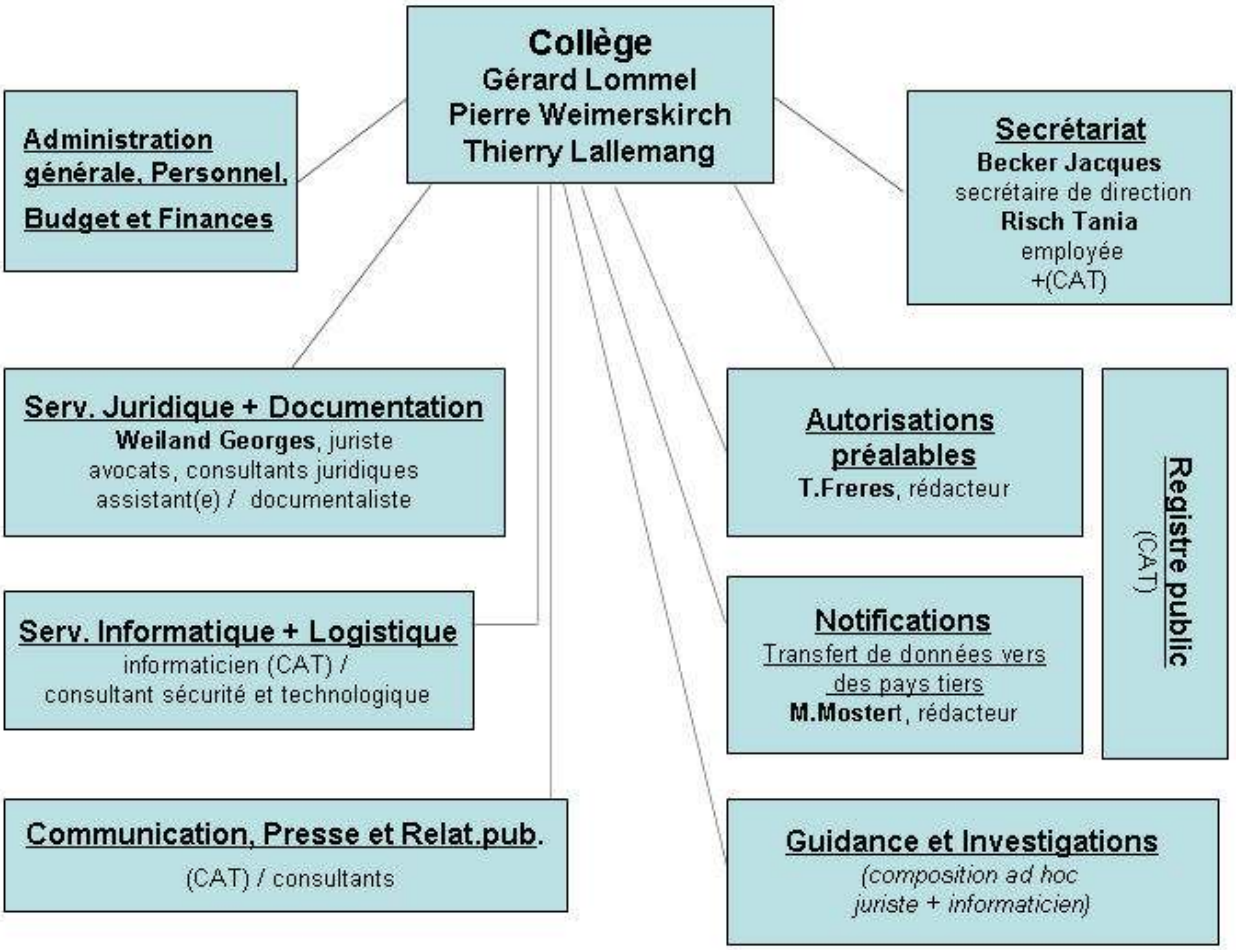
Par ailleurs les services ont été épaulé constamment par des auxiliaires mis à disposition par l'ADEM sous contrat CAT qui ont assurés (tant bien que mal compte tenu du taux de rotation élevé inhérent au statut en question) les fonctions d'assistant administratif et comptable, de juriste/documentaliste et d'informaticien.

Fait à Luxembourg, le 27 avril 2007

La Commission nationale pour la protection des données

(*s.*) Gérard Lommel Président	(*s.*) Pierre Weimerskirch Membre effectif	(*s.*) Thierry Lallemang Membre effectif

Organigramme de la CNPD



Feuille Couleur

IV. Annexe 1 : Statistiques

1) Formalités préalables

	2003	2004	2005	2006	
a) Notifications					**TOTAL**
- Notifications ordinaires :	2.646	850	500	250	4.246
- Notifications simplifiées :	750	900	720	890	3.260
(Total)	**3.396**	**1.750**	**1.220**	**1.140**	**7.506**
b) Autorisations préalables					
Demandes d'autorisation :	765	406	317	295	1.783
Engagements de conformité :	718	14	17	19	768
(Total)	**1.483**	**420**	**334**	**314**	**2.551**
c) Plaintes et requêtes diverses					
Plaintes demandes de vérification de licéité :	**15**	**38**	**40**	**30**	**123**
(Total général a) + b) +c))	**4.894**	**2.208**	**1.594**	**1.484**	**10.180**
Déclarants (responsables ayant accompli des formalités)	2.220	2.500	2.850	3.300	

2) Demandes de renseignements

	2004	2005	2006
a) Demandes de renseignements par courrier :			
- Administrations publiques	18	7	8
- Entreprises	49	10	8
- Professions libérales	3	4	9
- Citoyens	12	9	7
- Associations	7	5	2
(Total)	**89**	**35**	**34**
b) Demandes de renseignements par courriel :			
(Total)	**67**	**82**	**116**
c) Demandes de renseignements par téléphone :			
(Total)	**1.780**	**1.550**	**1.930**
(Total général a) + b) + c))	**1.936**	**1.667**	**2.080**

3) Séances de délibération

	2004	2005	2006
	39	36	39

4) Participations aux groupes de travail sur le plan européen

	2004	2005	2006
	28	33	23

5) Prises de contacts et concertations avec des organisations représentatives sectorielles ou acteurs

	2004	2005	2006
- Secteur public	47	62	32
- Secteur privé	30	38	12
(Total)	**77**	**100**	**44**

6) Séances d'information, conférences, exposés

	2004	2005	2006
	4	10	11

7) Séminaires

	2004	2005	2006
	6	13	8

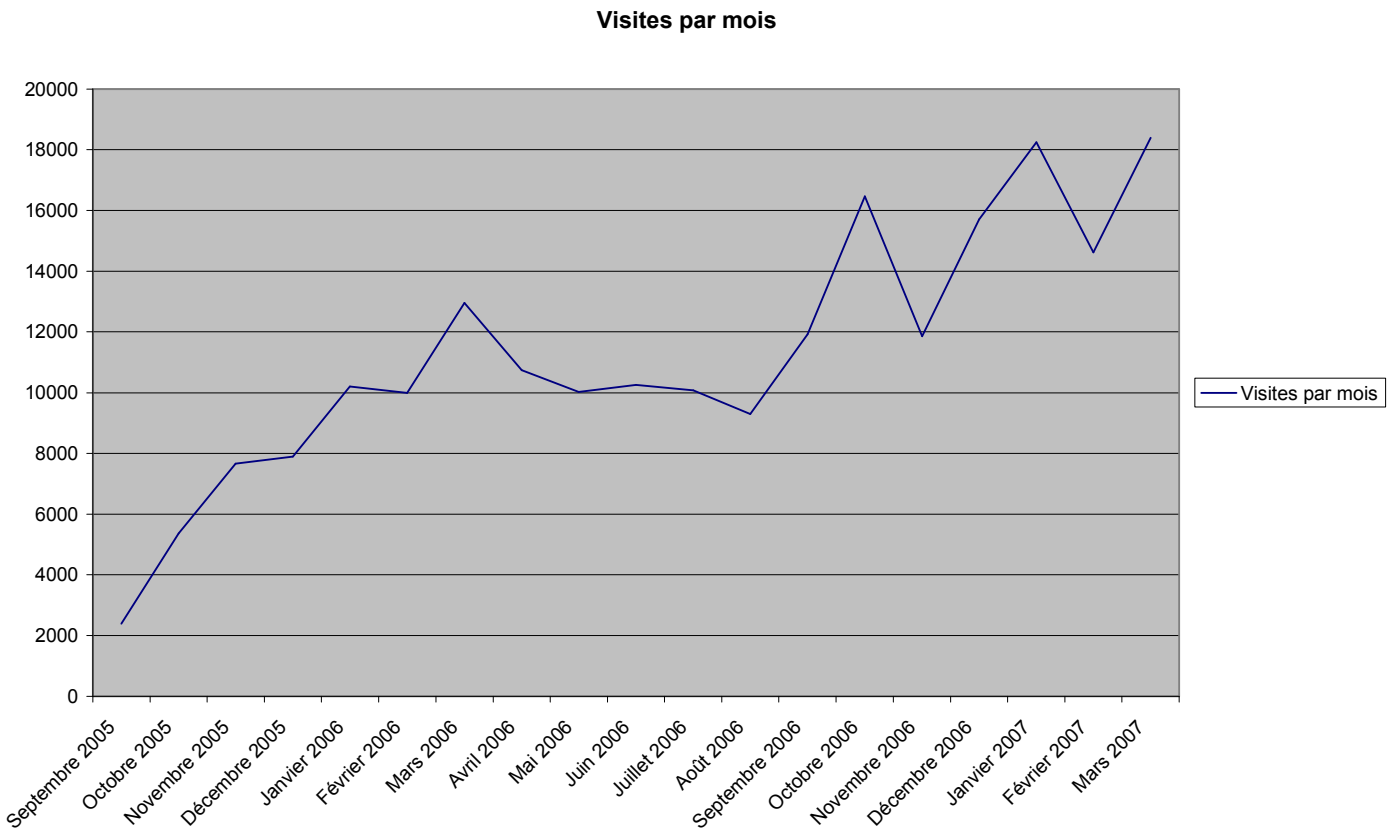
8) Campagne d'information du grand public

2004	Brochures
2005	Relaunch du site Internet / Brochures version portugaise
2006	Calendrier ULC / version anglaise du site

9) Reflets de l'activité de la CNPD dans la presse

	2004	**2005**	**2006**
Articles et interviews parus dans :			
- les quotidiens	14	16	67
- les hebdomadaires	5	6	4
- les mensuels	0	7	5
- les médias audiovisuels	1	3	3
(Total)	**20**	**32**	**79**

10) Fréquentations du site Internet



Feuille Couleur

V. Annexe 2 : Avis et décisions publiés

Avis de la Commission nationale pour la protection des données au sujet du projet de loi N°5181 relatif aux dispositions spécifiques de protection des personnes à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification de la loi du 2 août 2002

Délibération N°3/2004 du 20 février 2004

Conformément à l'article 32, paragraphe 3, lettre (e) de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, la Commission nationale pour la protection des données a entre autres pour mission d'« être demandée en son avis sur 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, et faisant suite à la demande lui adressée par courrier du 3 novembre 2003 de Monsieur le Ministre délégué aux Communications, que la Commission nationale entend présenter ci-après plusieurs observations, réflexions et commentaires au sujet des dispositions spécifiques du projet de loi 5181 relatives à la protection des personnes à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques (PARTIE I) et sur les dispositions portant modification de la loi du 2 août 2002 (PARTIE II). Elle a choisi de limiter ses observations aux questions ayant une incidence directe sur la protection des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel et notamment celle de la vie privée des personnes physiques.

PARTIE I. Avis relatif aux dispositions spécifiques de protection des personnes à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques

A. Conformité de la transposition

1) Champ d'application et définitions

Article 2

1) La distinction faite entre utilisateur et utilisateur final, introduite dans le projet de loi par égard à la législation sur les réseaux et les services de communications électroniques, n'a pas réellement lieu d'être dans le contexte de la protection de la vie privée. Il serait dès lors peut-être plus clair de n'utiliser que les notions d'utilisateur et d'abonné et de rayer en conséquence toutes les occurrences des termes « utilisateur final » du projet de loi.

2) Etant donné que la directive 2002/58/CE renvoie à la directive 95/46/CE pour définir le consentement, la Commission nationale renvoie de même quant à la notion de « consentement » (article 2 lettre c) du projet sous avis (calquée sur celle de la loi du 2 août 2002) à ses remarques formulées au niveau des modifications proposées à la loi du 2 août 2002 (ayant transposé la directive 95/46/CE) , telles que reprises sous la partie II, point 1) ci-après.

3) Il faudrait préciser que le terme d' « interconnexion » employé dans le projet sous avis, notamment à l' article 5, n'est pas à confondre avec la notion d'interconnexion visée à l'article 16 de la loi du 2 août 2002.

La présente notion d'interconnexion est celle est d'ores et déjà employée en matière de réseau de communications électroniques et en particulier, dans le nouveau paquet réglementaire communications électroniques.

Dans ce paquet, la directive 2002/19/CE du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion (directive « accès ») définit, en son article 2, l'interconnexion de la façon suivante :

« b) interconnexion : la liaison physique et logique des réseaux de communications publics utilisés par la même entreprise ou une entreprise différente, afin de permettre aux utilisateurs d'une entreprise de communiquer avec les utilisateurs de la même entreprise ou d'une autre, ou bien d'accéder aux services fournis par une autre entreprise. Les services peuvent être fournis par les parties concernées ou par d'autres parties qui ont accès au réseau. L'interconnexion constitue un type particulier d'accès mis en ouvre entre opérateurs de réseaux publics; »

On peut relever d'importantes différences entre ces deux utilisations d'une même terminologie :

- la directive 2002/19/CE parle d'interconnexion des réseaux et donc des moyens de communication quant la loi du 2 août 2002 parle de corrélation de données et donc de contenus ;
- la directive 2002/19/CE a comme champ les réseaux de communication publics quand la loi du 2 août 2002 couvre tant les réseaux publics que privés ;

Ainsi, ces utilisations de la terminologie d'interconnexion semblent être éloignées. En effet, a priori, l'une parle des moyens de communications quant l'autre parle de contenus corrélés (données à caractère personnel).

Cette distance n'est toutefois pas aussi marquée car la définition de la directive 2002/19/CE pose la question du contenu (qu'il s'agisse d'information à caractère personnel ou non).

En effet, la directive 2002/19/CE explique, après avoir défini l'interconnexion comme la mise en place physique de moyens permettant de communiquer entre deux réseaux auparavant distincts, qu'il peut également s'agir « d'accéder aux services fournis par une autre entreprise » et poursuit en disant que « Les services peuvent être fournis par les parties concernées ou par d'autres parties qui ont accès au réseau. ».

Ainsi, la directive 2002/19/CE, tout en parlant de liaison physique et logique, définit certains objectifs fonctionnels et en rapport au contenu (données à caractère personnel ou non).

Ces objectifs recoupent, pour les utilisateurs, la possibilité :

- de communiquer entre eux ;
- d'avoir accès à des services (contenus) pouvant, le cas échéant, être fournis par d'autres personnes que les opérateurs de réseau (par des prestataires de service) ;

Ces éléments fonctionnels nous rapprochent de la définition de la loi du 2 août 2002 qui, si elle concerne le contenu à caractère personnel, définit également l'interconnexion sous un aspect fonctionnel, c'est à dire celui d'une corrélation de données à caractère personnel.

De plus, une autre analogie peut-être faite. Les deux définitions permettent de qualifier d'interconnexion :

- concernant la directive 2002/19/CE, une opération concernant deux parties de réseaux d'un même opérateur
- ou encore, concernant la loi du 2 août 2002, deux traitements mis en œuvre par deux personnes responsables des deux traitements (qui en forment un troisième, à savoir, celui d'interconnexion).

De façon générale et introductive, il semble souhaitable de coordonner, lorsque c'est possible, les terminologies en provenance de diverses sources. Ceci est d'autant plus d'actualité que la réglementation des réseaux applique le principe de neutralité technologique et que la frontière contenu-contenant est de plus en plus ténue.

2) Sécurité : article 3

L'intitulé de l'article 3 du projet de loi pourrait préciser qu'il s'agit de la « Sécurité des services et des réseaux ».

Les termes « Sous réserve de ce qui précède » peuvent porter à confusion. En effet, il est difficile de déterminer si les fournisseurs de services et/ou les opérateurs ont l'obligation d'informer les abonnés quant aux mesures qu'ils peuvent prendre afin de rendre leurs communications sécurisées, en toutes circonstances ou uniquement lorsque les mesures qu'ils prennent eux-mêmes ne sont pas suffisantes.

Si la volonté du législateur est de limiter cette obligation au second cas, ce qui semble être l'orientation de la directive, il convient de remplacer « Sous réserve de ce qui précède » par « Si ces mesures ne sont pas suffisantes afin de remédier à l'atteinte à la sécurité ou pour en écarter le risque ».

3) Confidentialité des communications : article 4

L'article 4 du projet de loi transpose l'article 5 de la directive.

Article 4 paragraphe (2)

A noter que l'article 4 paragraphe (2) de la loi est cependant moins protecteur pour la personne concernée que l'article 5 paragraphe (1) de la directive.

La directive dispose que « en particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. »

En revanche, le projet sous avis prévoit qu' « il est interdit à toute personne autre que l'abonné, l'utilisateur ou l'utilisateur final concerné d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement de l'abonné, de l'utilisateur ou de l'utilisateur final concerné. »

Selon la formulation actuelle de l'article 4 paragraphe (2), il paraît donc possible que la confidentialité de la communication ne soit pas assurée entre l'abonné, l'utilisateur et l'utilisateur final dans la mesure où il s'agit de personnes différentes.

Si l'abonnée est une entreprise et l'utilisateur est son salarié, le projet sous avis laisse entrevoir la licéité d'une mesure de surveillance (écoute ou enregistrement) opérée par l'abonnée sur son salarié, qui est contraire à la confidentialité des communications prescrite par l'article 5 de la directive, et qui serait par ailleurs contraire tant à la loi du 11 août 1982 concernant la protection de la vie privée, qu'au régime d'autorisation institué par les articles 10, 11 et 14 de la loi du 2 août 2002.

Dans un souci de transposition fidèle de la directive, il faudrait supprimer les termes « abonné » et « utilisateur final », notions non prévues par la directive, laquelle définit à l'article 2 lettre a) le terme « utilisateur » comme étant « toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service ».

Article 4 paragraphe (3) lettre (c)

Aussi, les exceptions mentionnées à l'article 4 paragraphe (3) du projet de loi semblent bien appropriées, notamment eu égard au contenu des articles 10 et 15 paragraphe (1) de la directive. Quelques remarques importantes s'imposent malgré tout.

Il est fait mention de l'Institut à l'article 4 paragraphe (3) (c) et à d'autres endroits du projet de loi1. Il s'agit sans doute de l'Institut Luxembourgeois de Régulation (« ILR »), mais cela ne ressort pas clairement du texte du projet de loi. Peut-être faudrait-il définir l'Institut à l'article 2.

[1] Voir aussi les articles 5 (1) (a), 7 (5) et 9 (1) (a).

De plus, ce même article 4 paragraphe (3) (c) du projet de loi prévoit de permettre la réécoute de messages, la documentation de fausses alertes et la production de preuves. Or, ni le considérant 36, ni l'article 10 de la directive, ne visent le contenu des communications. Seules les données d'identification et de localisation de la ligne appelante sont visées et peuvent être utilisées dans le but précis de permettre aux services d'urgences d'intervenir le plus efficacement possible. S'il est concevable que la réécoute de communications en cas d'ambiguïté est néanmoins de nature à permettre une intervention plus efficace des services concernés et donc la défense et la sécurité publique au sens de l'article 15 de la directive, il n'en va pas de même en relation avec la production de preuves (puisque, par définition, l'intervention aurait déjà dû avoir lieu au moment de la production de ces preuves). Il n'est donc pas certain que cette dernière hypothèse soit couverte par la directive (à moins que l'on considère que les preuves recherchées le soient pour sauvegarder la sécurité nationale ou la poursuite d'infractions pénales, auquel cas l'article 15 de la directive trouverait également à s'appliquer).

La question des appels malveillants (fausses alertes, menaces et appels abusifs) est soulevée quand à elle par le considérant 36 de la directive qui ne mentionne cependant pour de tels appels que les données d'identification et non les données de localisation.

Le dernier alinéa de l'article 4 paragraphe (3) (c) du projet de loi n'est pas clair. Il mentionne les « données relatives au trafic y afférentes », sans qu'il soit fait référence à quoi ces données sont afférentes. Il conviendrait de remplacer cette phrase par « Les données relatives au trafic afférentes aux communications visées ci-dessus, y compris les données de localisation, doivent être effacées après l'intervention du service concerné (…) ». Cette formulation est au demeurant plus large et permet de viser tous les cas urgent, pas seulement les « secours » (notion qui n'est pas définie et donc source d'équivoque potentielle).

Enfin, en ce qui concerne la conservation du contenu des communications, et sous les réserves formulées ci-dessus à leur sujet, il conviendrait peut-être de préciser que le contenu des communications est à effacer après un délai de 6 mois « au plus », à moins que la volonté du législateur soit précisément de mettre à charge des opérateurs une obligation de conserver ces données pendant une durée fixée à 6 mois (auquel cas cela devrait être précisé).

Au même article 4 paragraphe (3) (c), deuxième alinéa, il conviendrait de mettre la proposition « dont les données de localisation » entre virgules.

Article 4 paragraphe (3) lettre (d)

L'article 4 paragraphe (3) (d) du projet de loi, qui constitue une exception au principe d'interdiction prévu à son article 4 paragraphe 2, devrait peut-être mentionner que l'abonné ou l'utilisateur concerné (et si cette distinction est maintenue, l'utilisateur final) est en droit de refuser le traitement envisagé, comme cela est prévu par la directive. Dans ce cas, par analogie avec la Directive 95/46/CE, il parait également indiqué de prévoir que le fournisseur de service ou l'opérateur doit avertir l'abonné concerné des conséquences d'un tel refus, notamment si le refus implique l'impossibilité de fournir le service demandé.

D'autre part, la Commission nationale salue l'initiative gouvernementale ayant libellé l'article 4 paragraphe (3) (d) du projet de loi de façon plus restrictive que la directive, car il ne mentionne que la possibilité d'effectuer des enregistrements pour fournir la preuve « d'une transaction commerciale » et écarte la fin de cette phrase « ou de toute autre communication commerciale », tel que prévu à l'article 5 paragraphe 2 de la directive.

La Commission nationale ne peut que partager cette approche prudente, puisque dans le cas contraire, en accordant aux responsables des traitements la possibilité supplémentaire d'effectuer des enregistrements pour fournir la preuve « à toute autre communication commerciale », le risque d'atteinte à la sphère privée se trouverait sensiblement aggravé pour la personne concernée (que ce soit le client ou le salarié de l'entreprise).

Quant à la dispense du « consentement »

L'article 4 paragraphe 3 point d) permet l'enregistrement d'une communication sans avoir obtenu le consentement des personnes concernées. Il constitue une exception au principe d'interdiction édicté à l'article 4 paragraphe 2.

En dépit du fait que la dispense du consentement est expressément consacrée à l'article 4 paragraphe 3 point d) du projet sous avis, la Commission nationale est d'avis que l'article 4 paragraphe 3 point d) reste en contradiction avec la loi du 11 août 1982 concernant la protection de la vie privée, en particulier avec son article 2 qui requiert le consentement de la personne enregistrée pour lever le voile de la confidentialité des communications privées.

Aux termes de l'article 2 de la loi précitée du 11 août 1982 :

« Est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 euros à 5.000 euros, ou d'une de ces peines seulement, quiconque a volontairement porté atteinte à l'intimité de la vie privée d'autrui.

1° en écoutant ou en faisant écouter, en enregistrant ou en faisant enregistrer, en transmettant ou en faisant transmettre, au moyen d'un appareil quelconque, des paroles prononcées en privé par une personne, sans le consentement de celle-ci;

2° en observant ou en faisant observer, au moyen d'un appareil quelconque, une personne se trouvant dans un lieu non accessible au public, sans le consentement de celle-ci, en fixant ou en faisant fixer, en transmettant ou en faisant transmettre dans les mêmes conditions l'image de cette personne.

Lorsque les actes énoncés au présent article ont été accomplis au cours d'une réunion au vu et au su de ses participants, le consentement de ceux-ci est présumé;

3° en ouvrant sans l'accord de la personne à laquelle il est adressé ou de celle dont il émane, un message expédié ou transmis sous pli fermé, ou, en prenant connaissance, par un appareil quelconque, du contenu d'un tel message ou en supprimant un tel message.

Les dispositions du No 1 du présent article ne s'appliquent pas à celui qui, chargé de l'entretien ou de la surveillance d'un réseau téléphonique public ou privé, écoute dans l'exercice de ses fonctions une communication pour s'assurer du bon fonctionnement de la liaison.

Est puni des peines prévues au présent article celui qui ne respecte pas le secret de la communication ainsi écoutée. »

Si l'intention du législateur était celle de déroger à la loi précitée de 1982 en ce qui concerne les communications effectuées au moyen d'un réseau de communication public et de services de communications électroniques accessibles au public, il parait préférable dans un souci de sécurité juridique de le mentionner expressis verbis dans le projet sous avis, à moins que le législateur ne retienne qu'une telle précision soit superflue au regard du principe général de droit que la loi postérieure (le projet sous avis) déroge implicitement à la loi antérieure (loi de 1982).

Cette conclusion s'impose davantage dans la mesure où l'article 1er du présent projet précise que les dispositions sont des dispositions spécifiques de « protection des données » applicables en matière de communications électroniques accessibles au public et qu'en dehors du champ d'application du présent projet, les dispositions générales de la loi du 2 août 2002 s'appliquent (document parlementaire 5181/00, p.12). Ceci est parfaitement en ligne avec l'article 1er paragraphe 2 de la directive 2002/58/CE qui dispose que « les dispositions de la présente directive *précisent et complètent* la directive 95/46/CE ». En revanche, rien n'est dit dans le projet sous avis quant à la loi de 1982, de sorte qu'il faut présumer que la volonté du législateur est celle de la laisser intacte.

Quant aux enregistrements à des fins de preuve des transactions commerciales, l'ABBL écrit dans son avis du 5 novembre 2003 que « *l'article 4 du projet de loi pose le principe de la confidentialité des communications. Il s'agit d'un texte spécial par rapport à la loi générale du 11 août 1982 concernant la protection de la vie privée qui, notamment, interdit l'écoute et l'enregistrement de communications sans le consentement des personnes concernées. Si la loi du 11 août 1982 sur la vie privée pose un tel principe, c'est parce qu'elle vise à protéger les interlocuteurs d'une communication contre l'enregistrement clandestin par des tiers. Elle ne dit rien cependant sur la situation d'une personne qui enregistre la communication téléphonique qu'elle entretient elle-même avec une autre personne. Il était donc urgent que cette situation soit clarifiée.* »

La Commission nationale ne saurait partager l'analyse de l'ABBL reprise à son compte par la Chambre de Commerce consistant à dire que la loi de 1982 ne préciserait pas si l'interdiction d'écouter, d'enregistrer ou d'intercepter les paroles prononcées en privé, au moyen d'un appareil quelconque, vise uniquement les tiers ou si cette prohibition doit être entendue comme s'appliquant également aux parties entre lesquelles les paroles prononcées en privé sont échangées.

En effet, en employant les termes de *« écoutant ou en faisant écouter, en enregistrant ou en faisant enregistrer »* la loi de 1982 fait envisage aussi bien le fait d'écouter ou d'enregistrer soi-même que le fait de « faire écouter ou enregistrer » par un tiers la conversation téléphonique. Quelle serait l'utilité et la signification de la distinction opérée si les parties à la conversation échappaient à la prescription légale?

Admettre que l'interdiction édictée à l'article 2 point 1 ne vise que les tiers revient à interpréter de la même façon le fait d'écouter/enregistrer ou de faire écouter/enregistrer, étant donné que dans cette logique « écouter/enregistrer » vise un premier tiers et « faire écouter/enregistrer » un deuxième tiers mandaté par le premier tiers. Or ces deux personnes sont des tiers par rapport à l'entretien téléphonique, de sorte qu'en visant à la fois deux personnes tierces différentes la distinction opérée par le texte légal en question ne donnerait aucun sens et ne serait qu'en réalité une redite superflue.

De même, en employant le terme « quiconque » la loi vise indistinctement le tiers à la communication privée et la partie concernée (partenaire de la conversation téléphonique) elle-même. Dans le cas contraire, le législateur aurait pris soin de préciser que la loi de 1982 vise uniquement les tiers et non aussi les partenaires à la conversation téléphonique. Or, tel n'est pas le cas.

En outre, cette interprétation de la loi de 1982 s'impose davantage à la lecture de la seconde phrase de l'article 2, point 2 : *« Lorsque les actes énoncés au présent article ont été accomplis au cours d'une réunion au vu et au su de ses participants, le consentement de ceux-ci est présumé; »*.

Est visée en l'occurrence la situation d'une réunion (d'affaires) où un enregistrement est effectué et les participants ayant été dûment informés. Dans cette hypothèse, si un participant à la réunion souhaite enregistrer la discussion, le consentement des autres participants est présumé lorsqu'il procède à l'enregistrement au vu et au su des autres.

La Commission nationale juge également opportun de rappeler ce qu'est une communication privée.

Dans le commentaire des articles relatif à la loi de 1982, l'on peut lire que « Il n'est pas nécessaire que ces paroles (prononcées par une personne en privé) aient été prononcées dans un lieu privé, même prononcée en un lieu public mais destinée à n'être entendue que par une personne déterminée, l'écoute de la conversation constitue une infraction » (doc. parl. 2177/00, p.1683).

Ceci rejoint l'approche du législateur belge, dont la loi luxembourgeoise de 1982 s'est inspirée.

D'après les travaux préparatoires de la loi belge, une communication professionnelle, mais non destinée à être entendue par d'autres personnes que les partenaires à la conversation est une communication privée au sens de la loi. Une communication est privée dans la mesure où elle n'est pas publique, et non pas dans le sens où elle ne serait pas professionnelle.

Contrairement à l'avis de l'ABBL du 5 novembre 2003 et de l'avis de la Chambre de commerce du 29 janvier 2003 (reprenant littéralement l'avis de l'ABBL sur ce point), la Commission nationale estime dès lors que l'employeur est à considérer comme étant tiers à la conversation téléphonique tenue entre son salarié et un client de l'entreprise, de sorte que le consentement et du salarié et du client est requise au titre de la loi de 1982, à moins que l'intention du législateur ne consiste à déroger à cette disposition d'ordre général en le précisant expressément dans le présent projet de loi.

Quant à la notion de « légalement autorisé »

La Chambre de Commerce a souligné dans son avis du 29 janvier 2004 que la « législation luxembourgeoise ne prévoit pas d'autorisation légale pour l'enregistrement des communications électroniques à des fins commerciales ».

Pour bien cerner la signification des termes « légalement autorisé », il y a lieu de rappeler la directive à cet égard :

Le considérant 23 de la directive 2002/58/CE prévoit que

« La confidentialité des communications devrait également être assurée dans les transactions commerciales licites. Au besoin et sous réserve d'une autorisation légale, les communications peuvent être enregistrées pour servir de preuve d'une transaction commerciale. La directive 95/ 46/CE est applicable en pareil cas. Les parties aux communications devraient être informées de l'enregistrement avant qu'il n'ait lieu, de la ou des raisons pour lesquelles la communication est enregistrée et de la durée du stockage de l'enregistrement. La communication enregistrée devrait être effacée dès que possible et, en tout état de cause, lors de l'expiration du délai légal de recours contre la transaction. »

L'article 5 paragraphe 2 de la directive dispose que :

« Le paragraphe 1 n'affecte pas l'enregistrement légalement autorisé de communications et des données relatives au trafic y afférentes, lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale. »

Il en découle qu'une autorisation par une disposition légale est nécessaire pour que l'exception au principe d'interdiction visée à l'article 4 paragraphe (3) (d) du projet sous avis puisse devenir efficace et trouver application.

Cette analyse de la directive 2002/58/CE est confirmée par l'autorité de contrôle belge en matière de protection des données.

« C'est cette intervention légale qui permettra de circonscrire les limites de l'exception au principe de confidentialité des données. Tant que l'exception prévue par la directive n'aura pas été explicitement transposée en droit belge, les responsables du secteur bancaire sont donc tenus d'obtenir le consentement des parties à la communication » (cf. avis n° 1/2002 du 22 août 2002 intitulé « Enregistrement des télécommunications effectuées dans le cadre des services bancaires », rendu par la Commission belge pour la protection de la vie privée).

Se pose la question de savoir si le législateur n'a pas d'ores et déjà créé cette « autorisation légale » en ayant introduit les articles 10 et 11 dans la loi du 2 août 2002 qui prévoient la possibilité une surveillance –notamment des conversations téléphoniques professionnelles- dans certaines conditions qu'ils ont pour objet de préciser. Il ressort d'ailleurs clairement des travaux préparatoires que l'hypothèse en question a été expressément envisagée.

« Relèvent également de la protection des biens de l'entreprise…(Art. 11 paragraphe (1) lettre b) … On peut encore y ajouter les écoutes téléphoniques effectuées par des établissements de crédit et autres professionnels du secteur financier aux fins d'enregistrer les ordres des clients passés par téléphone à condition toutefois que tant le client ait donné son accord à un tel enregistrement et que le salarié ait été informé que les conversations téléphoniques passées par ce téléphone seront enregistrées. (document parlementaire 4735/13, p. 21).

(1) Si tel est cas, l'enregistrement « légalement autorisé » vise donc l'article 10 paragraphe 1er lettre a) de la loi du 2 août 2002 prévoyant la possibilité d'enregistrement des conversations téléphoniques professionnelles moyennant le consentement (du client de la banque) et l'article 11 paragraphe 1er lettre b) de la loi du 2 août 2002 prévoyant cette possibilité pour la protection des biens de l'entreprise dans l'hypothèse où un salarié (de la banque) est partie à la conversation surveillée, l'autorisation préalable de la Commission nationale pour la protection des données étant requise par ailleurs en vue d'assurer le respect d'un juste équilibre entre les intérêts en cause.

(2) La Commission nationale rappelle dans ce contexte le rapport final de la commission des médias et des communications au niveau du projet de loi n° 4735 (ayant conduit à la loi du 2 août 2002) qui prévoit que : « *Il se peut qu'un même traitement tombe dans le champ d'application soit de l'article 10 soit de l'article 11 en fonction de la personne concernée. Par exemple, une caméra dans une grande surface tombe sous le coup de l'article 10 si la personne concernée est un client, même potentiel, du magasin et sous celui de l'article 11 si la personne concernée est un salarié employé par le propriétaire de ce magasin.*» (document parlementaire 4735/13, p. 17).

L'article 4 (2) du projet sous avis parle de « moyen d'interception ou de surveillance », de sorte que les articles 10, 11 et 14 de la loi du 2 août 2002 sont applicables au cas de figure de l'article 4 (3) sous avis.

Ainsi les paragraphes 2 et 3 de l'article 4 relatif à la confidentialité des communications sont parfaitement cohérents : une mesure de surveillance consistant dans l'enregistrement de communications n'est pas interdite dans le cadre des usages professionnels licites pour prouver une transaction commerciale, pourvu qu'une autorisation pour ce genre de traitements ait été octroyée au responsable du traitement par la Commission nationale en application des 10 et 11 de la loi.

Pour s'en tenir au libellé de l'article 4 paragraphe (3) (d) du projet sous avis : en raison de l'autorisation émise par la Commission nationale sur base de la loi du 2 août 2002 l'enregistrement a été « légalement autorisé ».

Dans cet ordre d'idées, la proportionnalité de la mesure de surveillance projetée sera appréciée au cas par cas par la Commission nationale.

(3) Dans le cas contraire, c'est-à-dire si l'on considère que les articles 10 et 11 de la loi du 2 août 2002 n'équivalent pas à l'autorisation légale requise au titre de la directive 2002/58/CE, la Chambre de Commerce relève à juste titre l'absence de texte légal mettant à profit l'exception prévue par la directive, de sorte qu'il incombe au législateur - bien évidemment s'il entend en faire bénéficier les milieux professionnels concernés - d'insérer dans le projet sous avis une disposition légale qui circonscrit précisément les limites de l'exception au principe de confidentialité des données en veillant à y appliquer les principes de transparence, de finalité, de nécessité et de proportionnalité ancrés dans la loi du 2 août 2002.

Finalement, la Commission nationale salue l'initiative gouvernementale consistant à réaffirmer dans l'article 4 § 3 lettre d) le principe du droit à l'information d'ores et déjà inscrit dans l'article 26 de la loi du 2 août 2002 et repris du considérant 23 précité.

Article 4 paragraphe (3) (e)

Pour éviter tout problème d'interprétation, la Commission nationale recommande de reprendre la teneur de la directive qui emploie le terme de « refuser » au lieu de « s'opposer » au niveau de l'article 4 paragraphe 3 lettre e).

Etant donné la collecte directe des données auprès de la personne concernée, la Commission nationale souligne que :

- les informations précises et complètes doivent être fournies au moment de la connexion, au moyen d'une communication selon la technique du « pop up » par exemple. Les méthodes retenues pour communiquer des informations doivent offrir un droit de refus ou solliciter le consentement (mais le consentement doit-il être exprès et non équivoque ?) ;
- les personnes concernées sont l'abonné, l'utilisateur ou l'utilisateur final. Cependant si l'accès à des terminaux appartient à des personnes morales abonnées, et lorsque plusieurs utilisateurs utilisent le service d'un même abonné, ou lorsqu'on est simplement en présence d'un abonné (tel un employeur) et d'un autre l'utilisateur (tel un employé), il est difficile à mettre en œuvre l'obligation d'informer et d'offrir le droit d'opposition requis. A titre d'exemple, il y a lieu de citer le problème de l'utilisation d'un équipement terminal par plusieurs utilisateurs, si un utilisateur accepte un cookie, celui-ci pourra être utilisé lors des sessions ultérieures initiées par d'autres utilisateurs.

Article 4 paragraphe (4)

Les sanctions prévues par l'article 4 paragraphe (4) du projet de loi semblent appropriées, notamment eu égard à l'article 24 de la directive 95/46/CE.

4) Données relatives au trafic : article 5

L'article 5 du projet de loi met en œuvre les possibilités offertes par les articles 6 et 15 de la directive de limiter la confidentialité des communications ou des données y afférentes.

Il semble que les critères et limitations de l'usage qui peut être fait des données soient appropriés par rapport aux conditions imposées par la directive. En effet, la conservation des données est limitée quant à son objet et quant à sa durée.

En ce qui concerne la durée de conservation, cette question est traitée séparément sous le point B du présent avis.

Article 5 paragraphe (1)

Peut-être faudrait-il préciser, à l'article 5 paragraphe (1) (b) du projet de loi que, à défaut d'être effacées, les données doivent être rendues anonymes « au sens de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel », c'est-à-dire de sorte à ne plus pouvoir identifier les personnes concernées.

Quant à l'article 5 paragraphe 1 lettre e), la Commission nationale relève que dans le domaine de la sécurité nationale, la défense et la sécurité publique ou dans le domaine de la prévention, recherche et poursuite d'infractions pénales la faculté pour les Etats-membres de déroger dans leur législation nationale au principe de finalité est contenu dans la directive 95/46/CE au niveau de l'article 13 qui permet de limiter la portée de l'article 6 paragraphe 1, lorsqu'une telle mesure s'avère nécessaire et est proportionnée au but recherché.

Article 5 paragraphe (2)

Il pourrait être utile, pour une simple question de langage, de remplacer « nécessaires à ce que de telles » par « nécessaires pour que de telles » et « de manière telle qu'il est impossible » par « de manière telle qu'il soit impossible ».

Article 5 paragraphe (3)

L'article 6 paragraphe (5) de la directive vise non seulement les traitements aux fins visées à l'article 6 paragraphe (3) de la directive (commercialisation de services et fourniture de services à valeur ajoutée) mais aussi les traitements aux fins visées à l'article 6 paragraphe (2) de la directive (facturation). Or, cela n'est pas prévu par l'article 5 paragraphe (3) du projet de loi.

Il serait par conséquent utile d'ajouter après la première phrase de l'article 5 paragraphe (3) du projet de loi que « L'abonné doit être informé des types de données relatives au trafic qui sont traitées [éventuellement ajouter aussi, par souci de cohérence avec le paragraphe suivant : « , de la finalité »] et de la durée du traitement ».

Par ailleurs, il serait peut-être avantageux de limiter la durée du stockage autorisé de données relatives au trafic à des fins de facturation ou de paiement pour interconnexion en fixant une limite maximale qu'il ne faudrait pas dépasser, sauf en cas de litige, les données n'étant plus nécessaires aux fournisseur de services ou à l'opérateur.

Dans ce cas, il conviendrait d'ajouter encore à la fin de l'article 5 (3), conformément à l'Avis 1/2003 sur le stockage des données relatives au trafic à des fins de facturation2 du Groupe de protection des données institué par l'article 29 de la Directive 95/46/CE (le « Groupe Article 29 ») : « (…) et ne peut en tout état de cause dépasser 6 mois lorsque la facture à été payée et n'a pas fait l'objet de litige ou de contestation ».

Article 5 paragraphe (4)

Il serait peut-être plus clair de remplacer « nonobstant son droit de pouvoir s'opposer à tout moment à un tel traitement » par « sans préjudice de son droit de retirer à tout moment sont consentement pour un tel traitement ».

Article 5 paragraphe (5)

Il faudrait peut-être viser le paragraphe (1) dans son ensemble plutôt que le paragraphe (1) (b) seul.

Article 5 paragraphe (6)

Les sanctions prévues par l'article 4 paragraphe (4) du projet de loi semblent appropriées. Malgré tout, il faudrait peut-être également viser le paragraphe (3), particulièrement si l'ajout suggéré plus haut est retenu. Dans ce cas, il faudrait simplement retirer les mots « des paragraphes (1), (2), (4), (5) ».

[2] Voir < http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp69_fr.pdf >.

5) Facturation détaillée

Il serait peut-être utile de faire référence, dans l'article 6 paragraphe (2) du projet de loi, à une liste de numéros qui ne devraient pas figurer sur les factures détaillées. En effet, l'article 6 (2) du Projet de Loi est limité aux appels gratuits et ceux aux services d'urgence et d'alerte. Or, d'autres numéros peuvent révéler des informations sensibles sur les personnes, comme par exemple les appels vers les services Aide aux femmes (12344), Aide aux victimes de la criminalité (40 20 40), Femmes battues (44 81 81), Info-viol (49 58 54). Une telle liste pourrait être maintenue à jour mise à la disposition des opérateurs par l'ILR.

6) Identification de la ligne appelante et de la ligne connectée

Article 7 paragraphe (1)

Outre la réserve émise ci-dessus quant à la distinction entre utilisateur et utilisateur final (voir point I. A. 1) Champ d'application et définitions) il faut remarquer que la dernière phrase de l'article 7 paragraphe (1) du projet de loi ne mentionne que l'abonné. Il faudrait ajouter la notion d'utilisateur (et d'utilisateur final si la distinction est maintenue).

Article 7 paragraphe (6)

Une erreur de frappe devrait être corrigée. A la place de « Les dispositions du paragraphe 1e s'appliquent », il faudrait lire « Les dispositions du paragraphe 1er s'appliquent ».

Article 7 paragraphe (8)

Il serait préférable de ne pas mentionner que l'abonné appelé prétendant être victime d'appel anonymes peut obtenir l'identification de la ligne appelante ou connectée. En effet, cela peut laisser supposer que la victime prétendue pourra dans tous les cas prendre connaissance de l'identification de la ligne appelante. Or, il est à supposer que, dans certains cas, il sera préférable que seuls les services de police ou les autorités compétentes concernées soient aptes à obtenir de telles données, notamment pour vérifier les assertions de victimes prétendues ou encore pour éviter qu'une victime n'utilise à son tour ledit numéro à mauvais escient. Il vaudrait donc mieux utiliser l'expression « peut demander l'identification » en lieu et place de « peut obtenir l'identification ».

A cet égard, il faudrait peut-être distinguer les cas d'appels réellement malveillants et ceux d'appels simplement dérangeants.

En tout état de cause, la disposition telle qu'elle est rédigée actuellement serait mieux compréhensible si les virgules avant et après l'expression « des appels répétés ou intempestifs » étaient retirées. Il faut encore remarquer que l'utilisateur (et l'utilisateur final) n'est pas visé par l'alinéa premier de cet article.

Pour plus de clarté, le deuxième alinéa de l'article 7 paragraphe (8) pourrait être modifié comme suit : « Un règlement grand-ducal fixera les modalités que devront respecter le fournisseur du service et/ou l'opérateur ainsi que l'abonné prétendant être victime d'appels anonymes à contenu malveillant. Il précisera également les caractéristiques d'un appel à contenu malveillant et déterminera les conséquences possibles de l'obtention par l'abonné ou les autorités compétentes de l'identification de la ligne appelante alors même que la présentation de cette identification avait été empêchée par l'abonné ou l'utilisateur appelant ».

7) Renvoi automatique d'appel

Peut-être faudrait-il aussi mentionner l'opérateur qui sera parfois le seul apte à fournir les données nécessaires pour faire cesser une déviation d'appel.

8) Données de localisation autres que les données relatives au trafic

Article 9 paragraphe (1)

La Commission nationale renvoie à ses commentaires faites sous le point B relatif à la durée de conservation.

Article 9 paragraphe (2)

Mêmes suggestions de modification que pour l'article 5 paragraphe (2).

Article 9 paragraphe (3)

La fin de ce paragraphe devrait être formulée comme suit : « (…) et sous réserve des dispositions des paragraphes (2), (4) et (5) ».

Par analogie avec l'article 5 paragraphe (4), il faudrait ajouter ensuite : « En ce qui concerne les traitements effectués avec des données qui ne sont pas rendues anonymes, l'abonné [seulement si cette distinction est maintenue : « , l'utilisateur »] ou l'utilisateur [« final »] peut à tout moment, gratuitement et sans indication de motif, retirer sont consentement ».

Relativement à des services à valeur ajoutée, il semble important de prévoir, à l'instar de l'article 9 de la directive, que, « En outre, l'abonné [seulement si cette distinction est maintenue : « , l'utilisateur »] ou l'utilisateur [« final »] doit être en mesure d'interdire temporairement, par un moyen simple et gratuit, le traitement des données de localisation autres que les données relatives au trafic le concernant ».

Article 9 paragraphe (4)

Ce paragraphe pourrait être reformulé de la manière suivante : « Le fournisseur du service et, le cas échéant, l'opérateur informent préalablement l'abonné, [seulement si cette distinction est maintenue : « , l'utilisateur »] ou l'utilisateur [« final »] des types de données de localisation autres que les données relatives au trafic qu'ils traitent, des finalités et de la durée de ce traitement ainsi que de la transmission éventuelle de ces données à des tiers en vue de la fourniture du service à valeur ajoutée. » La suite de la phrase devrait être supprimée, la question du consentement étant traitée au paragraphe précédent (voir ci-dessus, Article 9 (3)).

Article 9 paragraphe (5)

Même observation que pour l'article article 5 paragraphe (5) en ce qui concerne la référence au paragraphe (1) (b).

9) Annuaires d'abonnés

Voir plus particulièrement nos commentaires repris sous l'article 12 ci-après.

A l'article 10 paragraphe (1), la virgule qui suit « L'abonné » devrait être déplacée après « doit en être informé ».

10) Communications non sollicitées

Article 11 paragraphe (1)

L'article 11 paragraphe 1 transpose l'article 13 paragraphe 1 du texte de la directive 2002/58/CE.

L'envoi de courriers électroniques à des fins de prospection directe ne pourra intervenir que lorsque l'abonné aura préalablement consenti à cet envoi (consentement expresse et non équivoque).

Dans le cas où le responsable du traitement souhaite obtenir le consentement préalable de l'abonné par un des moyens visés par l'article 11 paragraphe 1er se pose indubitablement le problème de savoir si une telle demande en obtention du consentement préalable ne soit elle-même qualifiée de communication non sollicitée. Dans l'affirmative, le consentement doit être recueilli d'une autre manière.

Article 11 paragraphe (2)

Le début de l'article 11 paragraphe (2) devrait être ainsi libellé : « Sans préjudice du paragraphe (1er), le fournisseur qui, dans le cadre d'une vente d'un produit ou d'un service, (…) ».

Malgré tout, le terme fournisseur est vague puisqu'il n'est pas défini. De plus, il peut porter à confusion avec l'expression fournisseur de services qui, elle, est définie à l'article 2 du projet de loi et ne vise que les personnes qui fournissent des services de communications électroniques. Il conviendrait plutôt d'utiliser les termes « toute personne physique ou morale » proposés par la Directive et qui englobent aussi les personnes qui proposent des produits par le biais de services de communications électroniques.

Aussi, pour indiquer plus clairement que le fournisseur doit donner la possibilité à son client de refuser toute communication future, la formulation suivante serait indiquée : « (…) pour autant que ledit client soit clairement informé sur l'exploitation de ses coordonnées et se voit donner clairement et expressément la faculté de s'opposer par un moyen simple et gratuit à une telle exploitation (…) ». En effet, « nonobstant son droit de » indique simplement que le client à ce droit mais pas que le fournisseur doit le mettre expressément à sa disposition.

Enfin, même s'il est vrai que les termes « courrier électronique » sont ceux utilisés par la directive elle-même, il semble que les termes « message électronique » seraient plus appropriés car ils englobent également, sans équivoque, les services de messages courts (« SMS ») et de messages multimédias (« MMS »), seules les télécopies n'étant pas visées par cette disposition.

11) Dispositions transitoires et finales

Article 12 paragraphe (2)

Ici encore, le mot fournisseur est utilisé sans définition et peut porter à confusion avec la notion définie à l'article 2 du projet de loi de fournisseur de services.

Il faudrait en outre insérer l'idée que seuls sont visés les annuaires qui respectent les dispositions de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Cela pourrait être formulé comme suit : « Le fournisseur offrant un annuaire licite de „recherche inverse" (…) ». Sans cela, on pourrait penser que l'obtention éventuellement illicite de données serait validée par le silence de l'abonné.

La Commission nationale s'interroger sur la pertinence de cette disposition transitoire au regard des considérations suivantes.

Dans le commentaire des articles du projet de loi n° 5181, l'on peut lire sous l'article 10 que :

« Il convient que l'opérateur et/ou le fournisseur d'annuaires publics informent les abonnés figurant dans ces annuaires des fins auxquelles ceux-ci sont établis (paragraphe 1er) et de

toute utilisation particulière qui peut être faite des versions électroniques des annuaires publics, notamment grâce aux fonctions de recherche intégrées dans le logiciel, telles que les fonctions de recherche inverse qui permettent aux utilisateurs d'un annuaire de trouver le nom et l'adresse d'un abonné à partir d'un numéro de téléphone. Dans ce cas, il s'agirait d'une nouvelle finalité qui ne serait pas compatible avec la finalité primaire, et de ce fait en principe illicite selon le régime général de la loi du 2 août 2002 à moins que la personne concernée n'ait expressément consenti au traitement de ses données à ces nouvelles fins (paragraphe 3). Ainsi, le consentement informé des personnes concernées à l'inclusion de leurs données dans des annuaires publics pour des recherches inversées est donc indispensable. » (document parlementaire 5181/00, p.18 et 19).

La Commission nationale partage cette analyse qui se fonde sur les dispositions de l'article 14, paragraphe 1er, lettre (e) de la loi du 2 août 2002.

L'annuaire inversé constitue au sens de la directive 2002/58/CE du 12 juillet 2002 une utilisation des données à une fin autre que celle pour laquelle elle a été collectée, de sorte qu'en application de l'article 14, paragraphe 1er, lettre (e) de la loi, ce traitement est soumis à l'autorisation préalable de la Commission nationale, d'une part, et ne peut être effectué que moyennant consentement préalable de la personne concernée, d'autre part.

Il s'ensuit qu'au stade actuel de la législation luxembourgeoise, la situation visée par le second paragraphe de l'article 12 du projet sous avis qui réserve un « opt out » pour l'abonné (personne concernée) ne peut se rencontrer en pratique, alors qu'elle est d'ores et déjà contraire à la loi du 2 août 2002 en vigueur qui requiert le consentement exprès comme « opt in » pour utilisation des données pour une toute nouvelle finalité.

B. Durée de conservation des données

Le projet de loi fixe à 12 mois la durée pendant laquelle les fournisseurs de services et opérateurs sont tenus de conserver les données relatives au trafic et autres données de localisation.

Etant donné que la directive prévoit en son article 6 paragraphe (1), concernant la durée de conservation de les données relatives au trafic, que celles-ci « *doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaire à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1* ».

Que l'article 15 de la directive énonce que les Etats membres peuvent « *adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié* » pour la sauvegarde de la sécurité nationale, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et le poursuite d'infractions pénales.

Qu'en ce qui concerne les données de localisation autres que les données relatives au trafic, la directive dispose en son article 9 paragraphe (1) qu'elles ne peuvent être traitées « *qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée* ».

Qu'il n'est donc pas fait mention de l'article 15 de la directive comme à l'article 6 paragraphe (1) de la directive, mais l'article 15 de la directive lui-même permet de limiter la portée des droits et obligations de plusieurs dispositions, dont celles de l'article 9 de la directive.

On pourrait déduire de ces dispositions que les Etats membres ont toute latitude de prévoir une durée limitée pendant laquelle les fournisseurs de services ou les opérateurs seraient obligés de conserver toutes les données relatives au trafic et de localisation. C'est ce que fait le Projet de Loi en ses articles 5 paragraphe (1) (a) et 9 paragraphe (1) (a).

C'est la position qu'a adoptée la France dans la loi sur la sécurité quotidienne promulguée le 15 novembre 2001. Le principe d'effacement des données relatives à une communication y est inscrit, tempéré par deux exceptions : la conservation pour les besoins de facturation et la conservation à des fins de poursuite des infractions pénales, cette dernière ne pouvant dépasser un an. Des recommandations ont cependant été émises afin que la durée de conservation des données de communication soit réduite pour ce qui concerne la poursuite des infractions pénales.

A cet égard, l'annexe 2 du 9ème rapport sur la mise en œuvre de la réglementation de l'Union Européenne en matière de communications électroniques3 présente un tableau qui donne un panorama des dispositions législatives nationales existantes sur le sujet en Europe (voir page 32 dudit rapport).

Mais cette interprétation de la directive n'est pas la seule possible. En effet, d'aucuns considèrent que, dans l'état actuel des choses, les Etats membres ne peuvent pas prévoir a priori une durée de conservation généralisée des données relatives au trafic ou de localisation pour toutes les communications électroniques dont ils sont porteurs.

C'est notamment ce qui découle de la Déclaration des Commissaires européens à la protection des données adoptée lors de la conférence internationale de Cardiff du 9-11 septembre 2002, relative à la conservation systématique et obligatoire des données de trafic des télécommunications 4 : « *La protection des données de trafic dans les télécommunications est maintenant prévue dans la directive 2002/58/CE du Parlement européen et du Conseil concernant la vie privée et les communications électroniques (Journal Officiel L 201/37), qui précise que le traitement des données de trafic est en principe autorisé pour la facturation et le paiement des interconnexions. Après un très long et très explicite débat, il a été établi selon l'article 15 (1) de la directive que la conservation des données de trafic à des fins policières doit remplir des conditions strictes : dans chaque cas la conservation des données doit être prévue pour une période limitée et constituer une mesure nécessaire, appropriée et proportionnelle dans une société démocratique.*

Lorsque des données de trafic doivent être conservées, sa nécessité doit être démontrée, la période de conservation doit être aussi courte que possible et cette pratique doit être clairement établie par la loi, de façon à prévenir tout accès illégal ou tout autre forme d'abus.

La conservation systématique de tout type de données de trafic pour une période d'un an ou plus serait clairement disproportionnée et par conséquent inacceptable ».

[3] COM(2003) 715 final ; voir < http://www.europa.eu.int/information_society/topics/ecomm/doc/all_about/implementation_enforcement/annualreports/9threport/annex2181103.pdf >.

[4] Adoptée lors de la 24ème conférence internationale des commissaires européens à la protection des données personnelles qui s'est tenue à Cardiff au Pays de Galle du 9 au 11 septembre 2002) ; pour la déclaration complète, consulter < http://www.cnil.fr/thematic/docs/international/Cardiff_declaration.pdf >.

Cette position a été entérinée par le Groupe Article 29. En effet, dans son Avis 5/2002 sur la Déclaration des Commissaires européens à la protection des données adoptée lors de la conférence internationale de Cardiff du 9-11 septembre 2002, relative à la conservation systématique et obligatoire des données de trafic des télécommunications, adopté le 11 octobre 2002, le Groupe Article 29 déclare qu'il « *souscrit en tout point aux termes de cette déclaration* ».

Ainsi, si de nombreuses controverses ont précédé le vote de la Directive sur le sujet sensible de la rétention des données relatives au trafic, il ne s'agit apparemment pas actuellement pour les Etats membres de prévoir une conservation systématique des données, mais plutôt de prévoir un système « au cas pas cas »5.

Ce qui peut être prévu sans aucun doute, c'est la possibilité pour une autorité judiciaire nationale d'ordonner à un fournisseur de services ou à un opérateurs dans un cas particulier, par exemple dans le cadre d'une enquête judiciaire ouverte, de conserver exceptionnellement certaines données pendant une durée limitée, si cela est justifié par un motif énoncé à l'article 15 (1) de la Directive.

Ainsi, dans l'état actuel des choses, la Commission nationale estime que la règle devrait rester celle de l'interdiction de rétention des données de communications. Les exceptions doivent être verrouillées et permises uniquement dans un but précis, les mesures devant être nécessaires, appropriées, proportionnelles et prévues pour une durée limitée (la plus courte possible).

Un rapport sur la légalité de la rétention de données à l'égard des droits garantis par la Convention européenne des droits de l'homme confirme cette interprétation.

En effet, ce rapport expose que la notion de rétention systématique et généralisée de données à été rejetée expressément lors de l'adoption de la Directive.

Cependant, ce même rapport fait également état d'une décision-cadre, à l'étude au sein du Conseil de l'Union Européenne (Justice et Affaires Intérieures), qui imposerait aux Etats Membres de prendre des mesures législatives nationales pour obliger les fournisseurs de services et les opérateurs d'opérer une rétention de données pendant une durée allant de 12 à 24 mois pour les besoins éventuels d'enquêtes policières ou de poursuites judiciaires.

La rapport indique que de telles mesures seraient contraires aux dispositions de l'article 8 de la Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales, garantissant le droit à la vie privée, et de la jurisprudence de la Cour européenne des droits de l'homme (il y est fait référence dans le considérant 11 de la Directive).

Il paraît indiqué de rappeler la teneur de l'article 8 de la Convention européenne des Droits de l'Homme :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

Il en découle que la protection de la vie privée est la règle, et l'ingérence dans ce droit doit rester l'exception.

Plus récemment, le 9 janvier 2004, la Commission des libertés et des droits des citoyens, de la justice et des affaires intérieures du Parlement européen a publié un Projet de rapport

[5] D'aucuns considérant même qu'il en va « *de la défense des libertés fondamentales et constitutionnelles garanties également dans la Convention européenne des droits de l'homme* » (Marco CAPPATO, rapporteur sur la Directive) et du principe même de la démocratie

sur le premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE)6 (voir à la page 7).

Quant aux exceptions aux lois relatives à la protection de la vie privée, ce projet de rapport indique que le Parlement européen « *estime que les législations nationales prévoyant à des fins judiciaires la conservation sur une grande échelle de données concernant les communications entre citoyens ne sont pas pleinement conformes aux dispositions et à la jurisprudence de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, puisqu'elles instaurent un empiétement sur le droit à la vie privée qui n'est pas autorisé par le pouvoir judiciaire, au cas par cas et pour une durée limitée, qui ne distingue pas de catégories dans la population soumise à surveillance, qui ne respecte pas le secret des correspondances protégées (comme les communications de juriste à client), qui ne précise pas la nature des délits ni les circonstances qui justifieraient de tels empiétements, lesquels font naître en outre de sérieux doutes quant à leur nécessité pour une société démocratique ou à leur caractère approprié et proportionné – au sens de l'article 15 de la directive 2002/58/CE* ».

Par ailleurs, le projet de rapport indique également que le Parlement européen « demande à la Commission d'élaborer, sur la base de la convention européenne sur les droits de l'homme, de la jurisprudence qui en dérive et des directives sur la protection des données à caractère personnel, un document qui examine le droit à la vie privée et les exceptions légalement admises à ce droit et qui vérifie la conformité des mesures nationales de conservation des données personnelles ainsi que les lois nationales prévoyant des exceptions au principe général du droit à la protection de la vie privée pour des motifs comme l'ordre public, la défense nationale, la sûreté de l'État, ses intérêts économiques pourvu que des activités liées à la sûreté de l'État soient en jeu, la conduite de poursuites pénales, ou bien autorisant, pour les mêmes motifs, une interception de données à caractère personnel; invite les institutions européennes à lancer un débat ouvert et public au sujet dudit document ».

Dans ce contexte ambigu et en attendant les résultats des travaux actuels de l'Union européenne, la question pourrait être réglée par une disposition de type : « Rien dans la présente loi ne doit être interprété comme empêchant les autorités judiciaires compétentes d'ordonner aux fournisseurs de services ou aux opérateurs de conserver, pendant la durée qui leur sera indiquée, les données relatives au trafic ou de localisation concernant les communications qui leur seront désignées ». Il faudrait alors adapter les articles 5 paragraphe (1) (a) et 9 paragraphe (1) (a) du projet de loi.

Si le législateur devait malgré tout privilégier une interprétation de la directive lui permettant de fixer une durée pendant laquelle les données relatives au trafic doivent être systématiquement stockées par les fournisseurs de services ou les opérateurs, la Commission nationale est d'avis que la durée prévue actuellement de 12 mois constitue en tout état de cause le maximum acceptable.

Enfin, il y a lieu de réitérer les réserves formulées ci-dessus au sujet de la conservation de l'enregistrement du contenu des communications avec les services d'urgence prévu à l'article 4 paragraphe (3) (c) et limité à une durée de 6 mois (voir point A) 3).

[6] Voir < http://www.europarl.eu.int/meetdocs/committees/libe/20040121/519419fr.pdf >.

C. Lacunes potentielles

1) Article 14 de la Directive

Nous supposons qu'aucune mesure n'a été ou ne sera prise en vue d'imposer des exigences relatives à des caractéristiques techniques spécifiques aux terminaux ou autres équipements de communications électroniques et que cela n'est pas nécessaire pour les besoins de la transposition de la Directive.

2) Prospection directe – changement de régime – période de transition

Il est un point qui n'est pas traité par le Projet de Loi. En effet, on ne sait pas quel sera le sort des adresses de courrier électronique collectées licitement avant l'entrée en vigueur de la loi projetée.

Le système rendu obligatoire et retenu par le Projet de Loi en ce qui concerne la prospection directe par courrier électronique (médium le plus utilisé dans l'état actuel des choses) est celui du consentement préalable obligatoire (« opt-in »), avec possibilité permanente d'opposition (« opt-out »).

Est-ce à dire que les entreprises devront, suite à l'entrée en vigueur de la loi projetée, obtenir le consentement des personnes dont elles avaient déjà obtenu l'adresse électronique, par des investissements probablement très coûteux, et ce licitement sous l'empire de la loi 14 août 2002 relative au commerce électronique, amenée à être modifiée sur ce point par le projet de loi n° 5095 pour prévoir un système de opt-in ?

Il serait possible et peut-être raisonnable de prévoir une période de transition pour permettre aux fournisseurs de services disposant d'une base d'adresses de courrier électronique existante de contacter les personnes concernées afin de savoir si elles souhaitent ou non continuer à recevoir des courriers électroniques de prospection direct en provenance de ces fournisseurs de services.

II. DEUXIEME PARTIE : Avis sur les dispositions portant modification de la loi du 2 août 2002

A. Modifications prévues

Le projet de loi sous avis apporte à son article 12. – dispositions transitoires et finales sub (4) un certain nombre de modifications à la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Ces modifications visent d'une part à apporter certaines clarifications susceptibles d'éviter des difficultés d'interprétation et d'application des dispositions existantes et de compléter ces dernières sur des points mineurs d'autre part.

Par ailleurs l'article 11 est modifiée à son paragraphe 1er au point b de façon à marquer à l'abri de tout doute que cette condition de légitimité d'un traitement à des fins de surveillance sur le lieu du travail s'applique bien à tous les employeurs quelque soit leur statut, public ou privé.

Une condition de légitimité supplémentaire est ensuite rajoutée sous f) visant à autoriser l'employeur à surveiller – dans le respect des principes de nécessité et proportionnalité s'entend– ses travailleurs pour assurer la prévention, la recherche et la détection d'actes susceptibles d'engager la responsabilité de l'employeur.

Contrairement à ce que laisse entendre l'exposé des motifs. cette hypothèse s'appliquera aussi bien aux employeurs publics que privés et non seulement à l'Etat.

La Commission nationale s'interroge quant à la nécessité d'englober le terme « recherche» dans le libellé de ce point 11 §1f) nouveau alors que ceux de « prévention et détection » paraissent suffisants et mieux en harmonie avec les observations faites par le Conseil d'Etat au sujet de l'article 10 (document parlementaire 4735/3, p.15).

B. Réflexions supplémentaires

Pour le surplus elle marque son accord avec les modifications proposées. Elle exprime en outre ci-dessous un certain nombre de réflexions et soulève des questions rencontrées dans l'application de la loi qui pourrait le cas échéant conduire le gouvernement à envisager d'autres amendements à proposer.

1. Le consentement

La Commission nationale s'est d'abord posé la question de la conformité à la directive 95/46/CE (éventuel problème de transposition) de la notion de "consentement" telle que définie à l'article 2, lettre (c) de la loi qui s'écarte en partie de la rédaction de la définition contenue dans la directive.

Le législateur luxembourgeois a ajouté les adjectifs « expresse, non équivoque » à la notion de „consentement de la personne concernée" de l'article 2 lettre h) de la directive aux termes duquel le consentement est défini comme étant „toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement",

Si l'ajout du terme « non équivoque » peut encore s'expliquer au regard du terme « indubitablement » que l'on retrouve au niveau des articles 7 lettre a) et 26, paragraphe 1er lettre a) de la directive, il en va autrement du terme « expresse ». En effet, la directive emploie le terme « explicite » uniquement dans le contexte des traitements portant sur des catégories particulières de données (article 8 paragraphe 2 lettre a).

Il en découle que, contrairement à la directive, le législateur luxembourgeois ne permet pas au responsable du traitement de recourir à la condition de légitimité du consentement (article 5, paragraphe 1er, lettre f) de la loi) par une acceptation tacite, fût-elle non équivoque, des traitements qu'il entend mettre en œuvre portant sur des catégories particulières de données dans un contexte autre que celui où des traitements portent sur des catégories particulières de données.

Il va sans dire que les responsables des traitements souhaiteraient pouvoir faire état, du moins dans certaines hypothèses, d'un consentement implicite mais tacite comme critère de légitimation.

La loi nationale est donc sur ce point plus rigoureuse que la directive qu'elle entend transposer.

Par ailleurs, le législateur luxembourgeois ne fait pas de distinction entre le consentement requis en cas de données ordinaires et de données sensibles. Or, la directive opère une distinction sur ce point. Elle requiert le consentement explicite en ce qui concerne le traitement de catégories particulières de données, mais non pour les autres types de données à caractère personnel.

Pour se conformer pleinement à la directive, il nous semblerait préférable de supprimer le terme « expresse » au niveau de la définition du consentement et d'inclure le terme « explicite » à l'article 6, paragraphe 2 lettre a) de la loi du 2 août 2002 qui aurait dorénavant la teneur suivante :

« (a) la personne concernée a donné son consentement explicite *à un tel traitement, sauf indisponibilité du corps humain et sauf le cas interdit par la loi, ou lorsque* ».

Une telle adaptation de la loi nationale serait aussi de nature à rencontrer le souci exprimé par la Commission européenne dans son rapport publié le 15 mai 2003 sur la mise en œuvre de la directive 95/46/CE de voir réduire les divergences constatées dans les lois des Etats–membres, en particulier au niveau de la rédaction des définitions.

2. L'interconnexion

A) La notion d'"interconnexion" visée à l'article 2, lettre (j) de la loi devrait être clarifiée.

S'il est vrai que dans le projet de loi initial (cf. document parlementaire n°4735/00, page 2), l'interconnexion était définie comme étant "toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour une autre finalité par le même responsable du traitement ou par un ou d'autres responsables du traitement", il n'en reste pas moins que la Commission des Médias et des Communications

a adopté le 4 juillet 2002 un amendement au sujet de la notion d'interconnexion (cf. document parlementaire n° 4735/11, page 2) en la redéfinissant comme étant "toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d'autres responsables du traitement". C'est cette définition qui a été retenue en définitive par le législateur.

A la lecture du commentaire dudit document parlementaire, il appert qu' "il s*'agit d'une part d'assurer la consistance avec l'article 16 (3) qui vise des finalités identiques ou liées. D'autre part, comme la demande d'interconnexion doit émaner conjointement de plusieurs responsables de traitement, la référence à l'article 2 (j)* „au même responsable du traitement" a été supprimée. En effet, en cas de traitements ayant des finalités liées ou identiques effectués par un seul responsable du traitement, une notification unique ou une autorisation unique sont déjà prévues."

Il s'ensuit que l'on ne saurait parler d'interconnexion de données au niveau d'un seul et même responsable du traitement, alors qu'il convient de lire la définition visée sous l'article 2 lettre (j) comme étant toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par "un autre ou plusieurs autres" responsables du traitement.

A part le fait que la définition actuelle prête à confusion, la Commission nationale estime que cette définition est critiquable.

Un traitement issu de la corrélation, par une même personne, de données issues de deux autres traitements initiaux distincts devrait à notre avis être soumis au même régime qu'un traitement consistant en la corrélation, par deux personnes différentes.

Ces deux situations devraient être qualifiées l'une comme l'autre d'interconnexion au risque d'aboutir de façon injustifiée à deux régimes juridiques distincts, ceci, au détriment de la protection de la personne concernée et de façon discriminatoire.

De plus et en opportunité, les grandes sociétés et l'Etat, en tant que grands consommateurs de données à caractère personnel, sont particulièrement exposés à la tentation d'utilisation incompatible avec la finalité déterminée initiale. Or, le régime légal actuel libère bien trop souvent ces acteurs des règles applicables en cas d'interconnexion puisqu'ils pourront rattacher bon nombre de traitements au même responsable (le plus haut possible dans l'organigramme structurel) alors que s'ils considéraient chaque entité spécialisée comme responsable de ses traitements ils seraient bien souvent dans une hypothèse d'interconnexion. En revanche, les PME, professions libérales et individus n'ont pas la possibilité d'échapper à leur guise aux contraintes légales de l'interconnexion.

L'intérêt de la personne concernée ne saurait se satisfaire d'une solution discriminante offrant la protection adéquate seulement aux corrélations entre responsables distincts.

Le champ de l'interconnexion ne devrait pas donc être interprété comme excluant la corrélation de données issues de traitements ayant un seul et même responsable de traitement au risque de vider de son sens l'article 16 de la loi et de générer deux régimes a protection variable sans raison les justifiant.

En toute hypothèse, la CNPD devrait être attentive tant à la qualification de destinataire qu'à celle de responsable de traitement indiquée dans les dossiers de demande d'autorisation ou de notification.

En effet, de nombreux détournements de la loi semblent en perspective, surtout si le régime distinctif est appliqué. Les grandes institutions seront immanquablement tentées d'éviter l'article 16 en groupant tous leurs traitements sous un même chapeau de responsabilité or, selon l'article 2 (o) le responsable de traitement est : « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu des dispositions légales, le responsable du traitement est déterminé par ou en vertu des critères spécifiques conformément aux dispositions légales ».

La Commission nationale propose dès lors de reformuler la définition de l'interconnexion retenue à l'article 2 comme suit :

« (j) "interconnexion": toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité par un responsable du traitement *avec des données traitées dans d'autres traitements opérés par le même responsable du traitement ou par d'autres responsables du traitement* ».

Cette définition a également le mérite de régler un autre problème résultant du texte actuel. En ne visant que les traitements présentant entre eux des finalités identiques ou liées, la définition actuelle ne règle pas la situation d'une interconnexion de données traitées pour des finalités distinctes et non liées.

Si l'intention du législateur consistait à interdire en application de l'article 16 de la loi de telles interconnexions, il convient de ne pas les exclure de la définition retenue à l'article 2 lettre (j) de la loi et donc d'en biffer les termes « finalités identiques ou liées » .

C'est ainsi que l'article 16 paragraphe 3 de la loi trouvera pleinement application en posant comme condition sine qua non de licéité d'une interconnexion de données le respect de finalités identiques ou liées de fichiers. A contrario, sont prohibées au regard de l'article 16 paragraphe 3 les interconnexions des données traitées pour des finalités distinctes et non liées.

B) La Commission nationale relève par ailleurs qu'une interconnexion opérée par (le même ou) par différents responsables des traitements ne pourra être autorisée (par la loi ou la Commission nationale) que pour des traitements portant sur des finalités compatibles, tandis que le cas d'autorisation visé par l'article 14 paragraphe 1er lettre e) relatif à l'utilisation de données à des fins autres que celles pour lesquelles elles ont été collectées permet d'utiliser ultérieurement des données pour des finalités incompatibles.

3. La notion d'activités domestiques

L'article 3, paragraphe 5, de la loi dispose que celle-ci ne s'applique pas « au traitement mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques ».

Qu'en est-il de la surveillance sur le lieu de travail (soumise à l'autorisation préalable de la Commission nationale en vertu des articles 11 et 14) appliquée au travailleur domestique ?

La ratio legis doit amener la Commission nationale à décider qu'un tel traitement tombe bel et bien sous le champ d'application de la loi, puisqu'il ne s'agit pas à proprement parler d'une activité domestique du responsable du traitement, mais la personne physique occupant une femme de charge à son domicile privée est employeur et en cette qualité il met en œuvre un traitement à des fins professionnelles sujet à autorisation.

A supposer qu'une telle autorisation soit accordée, un problème peut se poser au niveau de l'exécution des missions incombant à la Commission nationale.

Aux termes de l'article 32, paragraphe (11) de la loi « Quiconque empêche ou entrave sciemment, de quelque manière que ce soit, l'accomplissement des mission*s incombant à la Commission nationale, est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. Est considéré comme empêchant ou entravant sciemment l'accomplissement des missions incombant à la Commission nationale, le refus opposé à ses membres de donner accès aux locaux autres que les locaux d'habitation, où a lieu un traitement aux données faisant l'objet d'un traitement ou de communiquer tous renseignements et documents demandés* ».

Concrètement, il n'y a pas de délit d'entrave pour le responsable du traitement qui refuse de donner accès à ses locaux d'habitation aux données faisant l'objet d'un traitement à des fins de surveillance de l'ouvrier domestique qu'il occupe. Est-ce possible que dans ce cas la notion de « local d'habitation » cède le pas à la notion de « lieu de travail » ?

Comment la Commission peut-elle en pareil cas exécuter sa mission fondamentale consistant à contrôler et à vérifier si les données soumises à un traitement sont traitées en conformité avec les dispositions de la présente loi et de ses règlements d'exécution ?

Il appartient au législateur de lever cette contradiction.

4. L'article 4, paragraphe (2) de la loi

Aux termes de l'article 4, paragraphe (2), les données traitées à des finalités déterminées peuvent être traitées ultérieurement à des fins historiques, statistiques ou scientifiques et sont soumises aux conditions prévues par le régime d'autorisation préalable de la Commission nationale tel que prévu à l'article 14.

Il serait utile d'intégrer dans ce paragraphe l'idée contenue dans le considérant 29 de la directive 95/46/CE qui énonce que « le traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques n'est pas considéré en général comme incompatible avec les finalités pour lesquelles les données ont été auparavant collectées, dans la mesure où les États membres prévoient des garanties appropriées; que ces garanties doivent notamment empêcher l'utilisation des données à l'appui de mesures ou de décisions prises à l'encontre d'une personne ».

Voir également en ce sens l'article 6, paragraphe 1, lettre b, de la directive aux termes duquel « …Un traitement ultérieur à des fins historiques, statistiques ou scientifique*s n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées* ».

La Commission nationale propose dès lors de donner la teneur suivante à l'article 4, paragraphe (2) de la loi :

« Un traitement ultérieur de données à *des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible avec les finalités déterminées pour lesquelles les données ont été auparavant collectées et est soumis aux conditions prévues par le régime d'autorisation préalable de la Commission nationale tel que prévu à l'article 14.* »

5. Les articles 6 et 7

A) Suivant l'article 6 paragraphe 4, lettre a) de la loi « Par dérogation à l'article 6, paragraphe (1), les données génétiques ne peuvent faire l'objet d'un traitement que dans les cas visés par les articles 6, paragraphe (2) lettres (c), (f), (g), (h), 6 paragraphe (3) et 7 de la présente loi ».

La Commission nationale émet les plus grandes réserves quant à l'opportunité de permettre - comme le prévoit le texte actuel - à tous les responsables des traitements visés à l'article 7 paragraphe 1 de la loi de traiter des données génétiques, étant donné que pour la majorité des instances y visées une telle faculté s'avère très dangereuse pour les « personnes concernées ».

En tout état de cause, la Commission nationale est d'avis que pour des raisons de non proportionnalité le traitement de données génétiques ne saurait se justifier dans le chef des entreprises d'assurances ou des sociétés gérant les fonds de pension. Il ne résulte d'ailleurs aucunement des travaux parlementaires pour quelles raisons ces acteurs économiques ont été ajoutés à la liste des « services de la santé » .

B) Suivant l'article 7, paragraphe (4) de la loi du 2 août 2002, sous réserve que leur traitement soit en lui-même licite au regard des articles 6 et 7, les données y visées peuvent être communiquées à des tiers ou utilisées à des fins de recherche, d'après les modalités et suivant les conditions à déterminer par règlement grand-ducal.

Aux termes de l'article 28-1, paragraphes 4 et 5, de la loi du 30 septembre 1992 modifiant la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques :

« (4) Un règlement grand-ducal pris sur avis du Conseil d'Etat détermine:

- les modalités d'après lesquelles les banques de données médicales peuvent être créées et exploitées;
- les modalités d'après lesquelles les données médicales peuvent être collectées et traitées;
- les conditions à observer afin de garantir la sécurité technique et le caractère confidentiel des données médicales collectées et traitées;
- les modalités d'après lesquelles les données médicales peuvent être communiquées à un tiers;
- les modalités d'après lesquelles les données médicales peuvent être utilisées à des fins de recherche.

Ce règlement peut aussi compléter les dispositions prévues aux chapitres 2 à 6 de la présente loi.

(5) La communication de données relatives à des prestations médicales, faite par le fournisseur de soins à un organisme de sécurité sociale aux *fins de remboursement des* dépenses afférentes est autorisée.»

Quant aux dispositions transitoires arrêtées dans la loi du 2 août 2002, celles-ci prévoient que:

« Avec l'entrée en vigueur de la loi, la loi modifiée du 31 mars 1979 réglementant l'utilisati*on des données nominatives dans les traitements informatiques est abrogée.*

Cependant „pour autant qu'ils ne sont pas contraires aux dispositions de la présente loi, les règlements pris en exécution de la loi modifiée du 31 mars 1979 précitée resteront en v*igueur tant qu'ils n'auront pas été remplacés par de nouvelles dispositions". Il s'agit de combler le vide juridique qui résulterait d'une abrogation expresse des règlements grand-ducaux pris en exécution de la loi modifiée du 31 mars 1979. Les règlements d'exécution, trouvant une base légale suffisante dans le nouveau texte, resteront en vigueur jusqu'à ce qu'il est pourvu à leur remplacement par de nouvelles dispositions »* (document parlementaire 4735/13, p. 45)

Il en découle que le paragraphe 5 de l'article 28-1 de la loi modifiée du 31 mars 1979 ayant pour objet d'autoriser le système du tiers payant se trouve abrogé depuis le 1er décembre 2002, date d'entrée en vigueur de la nouvelle loi du 2 août 2002, sans qu'une nouvelle base légale n'ait été créée en échange.

Dans ces circonstances il paraît urgent de voir pallier à cette lacune. Le législateur entendait sans doute que ceci se ferait dans le cadre du règlement grand-ducal prévu à l'article 7 paragraphe (4) de la loi du 2 août 2002 appelé à déterminer les modalités et les conditions suivant lesquelles les données visées aux articles 6 et 7 peuvent être communiquées à des tiers ou utilisées à des fins de recherche, sous réserve que leur traitement soit en lui-même licite. Ce règlement n'est cependant pas encore intervenu. Il est vrai que l'article 44 paragraphe (2) dispose que les règlements d'exécution de l'ancienne loi trouvant une base légale suffisante dans le nouveau texte resteront en vigueur jusqu'à ce qu'il soit pourvu à leur remplacement par de nouvelles dispositions et a explicitement visé à ce titre le règlement grand-ducal du 2 octobre 1992 réglementant l'utilisation de données nominatives médicales dans les traitements informatiques. Or ce règlement ne règle pas la communication de données relatives à la santé dans le cadre du système du tiers payant, puisque ceci faisait l'objet d'une disposition légale expresse.

Quant aux conditions générales pour la communication de données médicales à des tiers prévues au chapitre IV de ce règlement grand-ducal du 2 octobre 1992 réglementant l'utilisation de données nominatives médicales dans les traitements informatiques, elles donnent lieu à une difficulté supplémentaire. L'article 16 (2) prévoit en effet que « *le consentement écrit n'est pas requis lorsque l'intérêt direct du malade exige la communication et qu'il y a lieu de présumer le consentement* » Il apparaît douteux en effet que la notion de consentement présumé » soit compatible avec la définition du consentement de la loi du 2 août 2002. En outre l'hypothèse envisagée présuppose que la personne concernée puisse être considérée comme « malade » et a recours à la notion d'intérêt direct non définie par ailleurs et nettement plus large que celle de « sauvegarde de l'intérêt vital » employée par la loi du 2 août 2002 aux articles 5 paragraphe 1er lettre(e) et 6 paragraphe (2) lettre (c)

Une clarification semble donc s'imposer, soit par la voie d'un règlement grand-ducal à prendre conformément à l'article 7 paragraphe (4) de la loi du 2 août 2002 appelé à déterminer les modalités et les conditions suivant lesquelles les données visées aux articles 6 et 7 peuvent être communiquées à des tiers ou utilisées à des fins de recherche, soit par de nouvelles dispositions venant compléter la loi à ce sujet.

6. L'article 9 : liberté d'expression

Concernant les modifications proposées à l'article 9, la Commission nationale renvoie à son avis substantiel émis dans le cadre du projet de loi n° 4910 sur la liberté d'expression dans les médias (cf. document parlementaire n° 4910/09).

7. L'article 10

A) Aux termes de l'article 10, paragraphe 1er, lettre (a) le traitement à des fins de surveillance peut être autorisé si la personne concernée a donné son consentement.

Les travaux parlementaires ne donnent aucun exemple pour cette condition de légitimité.

Si cette condition de légitimité peut certes viser l'hypothèse du client donnant son accord pour l'enregistrement des conversations téléphoniques avec sa banque afin de permettre à cette dernière de prouver des transactions commerciales, elle cadre mal avec le cas du malade (inconscient) se trouvant dans l'incapacité physique de donner son consentement mais qui est mis sous (vidéo) surveillance continue, en particulier en cas de réanimation médicale.

Un autre cas visé pourrait être celui des personnes dangereuses placées sous vidéosurveillance par exemple en garde à vue dans un milieu neuro-psychiatrique ou pénitentiaire enfermées dans un cabanon (« *Gummizelle* »).

A notre sens, on devrait également reprendre au niveau de l'article 10 (1) lettre a) le cas de figure réglé à l'article 6 paragraphe 2 lettre c) qui couvre les hypothèses où des données relatives à la santé sont traitées en dehors du contexte de la surveillance. La Commission nationale propose donc à cet effet de rajouter au paragraphe 1ier de l'article 10 un point d) libellé comme suit :

(d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapa*cité physique ou juridique de donner son consentement.*

B) De l'avis de la Commission nationale, les notions de « sécurité des usagers » et « prévention des accidents » inscrites à l'article 10, paragraphe 1, lettre (b) n'englobent pas le cas des actes de vandalisme (dans les bus ou dans les gares etc.) ou les vols de biens.

Dans un souci de cohérence au niveau des articles 10 et 11 de la loi, il apparaît cependant que ces hypothèses peuvent constituer des causes légitimes de recours à des traitements à des fins de surveillance.

La Commission nationale propose dès lors de modifier le texte légal en conséquence en ajoutant « la protection des biens » sous l'article 10, paragraphe 1er lettre b), pour y inclure notamment les vols ou les actes de vandalisme, d'autant plus que cette situation est d'ores et déjà réglée sous la lettre b) du premier paragraphe de l'article 11 relatif aux traitements à des fins de surveillance sur le lieu de travail.

8. L'article 11

La Commission nationale estime en revanche qu'il convient de biffer les termes « de l'entreprise » au niveau de l'article 11 § 1 lettre b), au motif qu'il existe encore d'autres personnes intéressées que l'employeur dont les biens méritent une protection, protection qui pourrait constituer une condition de légitimité au titre de la surveillance envisagée sur le lieu de travail. (Cette observation vaut également pour le nouveau libellé prévu dans le projet de loi sous avis : « *quelque soit le statut, public ou privé, de l'employeur* »).

En effet, comme la condition de légitimité indiquée sous le point b) du premier paragraphe de l'article 11 couvre exclusivement un traitement à des fins de surveillance sur le lieu de travail « pour les besoins de protection des biens de l'entreprise », il en découle nécessairement « a contrario » que les biens appartenant aux autres salariés qui sont déposés dans leur vestiaire personnel ne sont pas couverts par cette condition de légitimité en cas de vol perpétré par un de leurs collègues de travail.

En pareil cas, l'employeur ne peut faire bénéficier son salarié, victime du vol, des preuves collectées par un appareil pour lequel il a obtenu une autorisation pour protéger ses propres biens.

9. L'article 14

Dans le cadre du projet de loi n° 5181, il conviendrait également prévoir pour les engagements formels de conformité (pris en application de l'article 14, paragraphe 3, de la loi) au niveau du nouveau paragraphe 5 du même article la perception d'une redevance à fixer par règlement grand-ducal.

Le tarif serait sans doute plus modeste pour tenir compte de l'article 37, paragraphe 4, de la loi aux termes duquel :

« *La Commission nationale est autorisée à prélever la contrepartie de ses frais du personnel en service et de ses frais de fonctionnement par la redevance à percevoir telle que prévue à l'article 13 de la présente loi. Pour le solde des frais restant à couvrir dans le cadre de ses missions conférées par la présente loi, la Commission nationale bénéficiera d'une dotation d'un montant à déterminer sur une base annuelle et à inscrire au budget de l'Etat.* »

10. L'article 15

Aux termes du premier paragraphe de l'article 19 de la directive 95/46/CE „les Etats membres précisent les informations qui doivent figurer dans la notification qui comprennent entre autres au minimum le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant.

L'article 13, paragraphe 1er de la loi du 2 août 2002 prévoit en outre l'indication du sous-traitant.

Comme les clients des experts-comptables et réviseurs d'entreprises par exemple devront indiquer ces professionnels dans leurs notifications comme sous-traitants, la publicité conférée de cette manière à ces informations par le biais du registre public des traitements en ligne permettrait de reconstituer les bases de clientèle de chaque cabinet luxembourgeois de révision et d'expert-comptable.

Dans un souci de sauvegarder la confidentialité de la clientèle des professionnels en cause, nous suggérons donc de supprimer le bout de phrase relatif au sous-traitant au niveau du premier paragraphe.

11. L'article 26 : le droit à l'information de la personne concernée

Le « droit à l'information de la personne concernée » est réglementé par l'article 26 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel qui prévoit en son paragraphe 1er lettre c) (lorsque les données sont collectées directement auprès de la personne concernée):

« *(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 la concernant et de rectification de ces données;
- la durée de conservation des données. »

Le paragraphe 2 lettre c) (lorsque les données n'ont pas été collectées auprès de la personne concernée) du même article dispose :

« *(c) toute information supplémentaire telle que:*

- les catégories de données concernées;
- les destinataires ou les catégories de destinataires des données auxquels les données sont susceptibles d'être communiquées;
- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;
- la durée de conservation des données. »

Le législateur luxembourgeois s'est inspiré de la rédaction de la directive 95/46 CE du Parlement Européen et du Conseil du 24 octobre 1995 en reprenant aux paragraphes (1) et (2) de l'article 26 presque textuellement les deux modalités d'information de la personne concernée visées aux articles 10 et 11 de la directive (doc. parl. 4735/13 p. 23). Les articles 10 et 11 règlent la question de l'information en cas de collecte de données de la manière suivante :

Article 10

Informations en cas de collecte de données auprès de la personne concernée

Les États membres prévoient que le responsable du traitement ou son représentant doit fournir à la personne auprès de laquelle il collecte des données la concernant au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée:

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

b) les finalités du traitement auquel les données sont destinées;

c) toute information supplémentaire telle que :

- les destinataires ou les catégories de destinataires des données,

- 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 la 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.

Article 11

Informations lorsque les données n'ont pas été collectées auprès de la personne concernée

1. Lorsque les données n'ont pas été collectées auprès de la personne concernée, les États membres prévoient que le responsable du traitement ou son représentant 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 au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée:

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

b) les finalités du traitement;

c) toute information supplémentaire telle que:

- les catégories de données concernées,

- les destinataires ou les catégories de destinataires des données,

- l'existence d'un droit d'accès aux données la 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.

2. Le paragraphe 1 ne s'applique pas lorsque, en particulier pour un traitement à finalité statistique ou de recherche historique ou scientifique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si la législation prévoit expressément l'enregistrement ou la communication des données. Dans ces cas, les États membres prévoient des garanties appropriées.

Quant à l'étendue de l'obligation d'information, il résulte clairement des articles 10 et 11 que les informations tombant dans la catégorie « toute information supplémentaire » ne doivent être fournies à la personne concernée que « 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 directive pose ainsi le principe de nécessité applicable en la matière en fonction du traitement mis en œuvre par le responsable du traitement.

Force est de constater que la loi luxembourgeoise est moins flexible en ayant omis de transposer également le bout de phrase « 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 ».

S'il est vrai que l'on peut et doit interpréter et appliquer l'article 26 à la lumière des articles 10 et 11 de la directive, toujours est-il qu'un ajout légal au texte actuel enlèverait un élément d'insécurité juridique quand à la lecture qu'il convient de faire de ce texte qui ne donnerait plus ainsi lieu à des critiques éventuelles.

D'ailleurs, il résulte des travaux parlementaires que l'intention du législateur était dictée par les mêmes considérations de souplesse que celles inscrites à la directive.

« Le responsable du traitement devra fournir toutes les informations supplémentaires nécessaires, compte tenu des circonstances particulières dans lesquelles les données sont collectées, pour assurer à l'égard de la personne concernée un traitement loyal des données, c'est-à-dire une information pleine et entière. La liste de ces informations supplémentaires n'est pas exhaustive. Ainsi, par exemple, si les données n'ont pas été fournies par la personne concernée, celle-ci peut, suivant les cas, être en droit de connaître l'identité de la personne ayant fourni des données la concernant. De même l'article 30, paragraphe (1) lettres (b) et (c), oblige le responsable du traitement à informer la personne concernée de l'existence d'un droit d'opposition en cas de traitement à des fins de prospection. » (document parlementaire 4735/13, p. 24).

Les lettres c) du paragraphe 1er et 2 de l'article 26 de la loi auraient dorénavant la teneur suivante :

Le paragraphe 1er lettre c) :

« (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 la concernant et de rectification de ces données;

la durée de conservation des 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. »

Le paragraphe 2 lettre c) :

« (c) toute information supplémentaire telle que:

- les catégories de données concernées;
- les destinataires ou les catégories de destinataires des données auxquels les données sont susceptibles d'être communiquées;
- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;

la durée de conservation des 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»

L'article 32

Conformément à l'article 32, paragraphe 7, la Commission nationale dispose d'un pouvoir d'investigation en vertu duquel elle a accès aux données faisant l'objet du traitement en question.

Elle recueille toutes les informations nécessaires à l'accomplissement de sa mission de contrôle. A cette fin elle a un accès direct aux locaux autres que les locaux d'habitation où a lieu le traitement ainsi qu'aux données faisant l'objet du traitement et procède aux vérifications nécessaires.

La CNPD regrette cependant que cet article omet de préciser si les membres de la CNPD ont la qualité d'officiers de police judiciaire, ou si la CNPD peut requérir les forces de l'ordre pour l'assister dans l'accomplissement de ses missions légales.

Dans la négative, il faudrait l'ajouter à cet article, et ce indépendamment du fait que le délit d'entrave est visé à l'article 32 paragraphe 11 disposant que « Est considéré comme empêchant ou entravant sciemment l'accomplissement des missions incombant à la Commission nationale, le refus opposé à ses membres de donner accès aux locaux autres que les locaux d'habitation, où a lieu un traitement aux données faisant l'objet d'un traitement ou de communiquer tous renseignements et documents demandés. »

Dans ce contexte, le législateur pourrait notamment s'inspirer de la loi du 8 septembre 1998 réglant les relations entre l'Etat et les organismes oeuvrant dans les domaines social, familial et thérapeutique qui dispose en son article 9 :

« Chaque ministre prévu à l'article 1er de la présente loi est chargé, pour les activités qui le concernent, de surveiller et de contrôler la conformité de ces activités avec les dispositions de la présente loi.

Dans le cadre de sa mission de surveillance et de contrôle chaque ministre désigne un ou plusieurs fonctionnaires de l'Etat, soit de la carrière supérieure soit de la carrière moyenne relevant du cadre fermé, avec la mission de rechercher et de constater des infractions à la présente loi et à ses règlements d'exécution, le tout sans préjudice des pouvoirs reconnus aux officiers et agents de police judiciaire de la gendarmerie et de la police.

Dans l'exercice de leurs fonctions relatives à la présente loi, les fonctionnaires visés ci-avant ont la qualité d'officier de police judiciaire. Ils constatent les infractions par des procès-verbaux faisant foi jusqu'à preuve contraire. Leur compétence s'étend sur tout le territoire du Grand-Duché.

Avant d'entrer en fonctions, ils prêtent devant le tribunal d'arrondissement de leur domicile le serment suivant: «Je jure de remplir mes fonctions avec intégrité, exactitude et impartialité.»

L'article 458 du code pénal leur est applicable.

Les fonctionnaires prévus ci-avant ont accès aux locaux, terrains et moyens de transport des personnes et organismes assujettis à la présente loi. Ils peuvent pénétrer même pendant la nuit, lorsqu'il existe des indices graves faisant présumer une infraction à la présente loi, dans les locaux, terrains et moyens de transport visés ci-dessus. Ils signalent leur présence au chef de l'organisme ou à celui qui le remplace. Celui-ci a le droit de les accompagner lors de la visite. »

Une autre alternative consisterait à intégrer la faculté pour la Commission nationale de requérir la force publique en cas de besoin, telle que prévue à l'article 13 de la loi du 4 avril 1974 portant réorganisation de l'Inspection du travail et des mines :

« S e c t i o n 1. - Pouvoirs du personnel

Art. 13. (1) Le personnel d'inspection et le personnel de contrôle muni de pièces justificatives de ses fonctions est autorisé :

a) à pénétrer librement sans avertissement préalable, à toute heure du jour et de la nuit dans tout établissement assujetti au contrôle de l'inspection du travail; le droit de libre accès s'étend à toutes les dépendances des entreprises;

b) à pénétrer le jour dans tous les locaux qu'il peut avoir un motif raisonnable de supposer être assujettis au contrôle de l'inspection du travail et des mines.

Les dispositions du présent paragraphe ne sont pas applicables aux locaux qui servent à l'habitation.

(2) Lorsque le personnel visé au paragraphe (1) qui précède rencontre des difficultés à l'occasion de ses visites, il peut requérir les chefs locaux de la gendarmerie et de la police qui lui prêteront main forte.

(3) A l'occasion de l'exercice des droits visés au paragraphe (1) qui précède, le personnel d'inspection et le personnel de contrôle est tenu d'informer l'employeur ou son représentant ainsi que le président de la délégation ouvrière et, le cas échéant, le président de la délégation des employés de l'entreprise de sa présence.

(4) Il n'en est pas ainsi toutefois lorsqu'il estime que l'information prévue à l'alinéa qui précède risque de porter préjudice à l'efficacité du contrôle; dans ce dernier cas, le directeur de l'inspection du travail, ou, en cas d'empêchement, «l'un des directeurs adjoints»1 devra en être informé préalablement. »

L'article 36

L'étendue des missions de la Commission nationale, en particulier celles comportant de vastes et complexes recherches juridiques, l'élaboration d'avis et de recommandations ainsi celles relatives aux mesures de sécurité à respecter par les responsables des traitements, le recrutement à un stade à déterminer d'un juriste et d'un informaticien (ingénieur diplômé ou ingénieur technicien) auprès de la Commission nationale sous le statut de fonctionnaire s'impose afin de garantir le bon fonctionnement de l'établissement public.

Par conséquent, le cadre du personnel de la Commission nationale doit être étendu aux fonctions et emplois suivants :

« a) dans la carrière supérieure de l'attaché de direction:

- des conseillers de direction 1ère classe ou
- des conseillers de direction ou
- des conseillers de direction adjoints ou
- des attachés de direction 1ers en rang ou
- des attachés de direction.

b) dans la carrière supérieure de l'ingénieur:

- des ingénieurs 1ère classe;
- des ingénieurs chef de division;
- des ingénieurs principaux ou ingénieurs-inspecteurs ou ingénieurs;»

c) dans la carrière moyenne de l'ingénieur technicien:

- des ingénieurs techniciens inspecteurs principaux premiers en rang;
- des ingénieurs techniciens inspecteurs principaux;
- des ingénieurs techniciens inspecteurs;
- des ingénieurs techniciens principaux;
- des ingénieurs techniciens. »

L'article 37 paragraphe 4

En raison du fait que le projet de loi (n° 5181) prévoit également la perception d'une redevance pour les demandes d'autorisation préalable à introduire auprès de la Commission nationale, il convient de mentionner l'article 14 à l'article 37 paragraphe 4 de la loi, paragraphe qui aurait dorénavant la teneur suivante :

«(4) La Commission nationale est autorisée à prélever la contrepartie de ses frais du personnel en service et de ses frais de fonctionnement par la redevance à percevoir telle que prévue aux articles 13 et 14 de la présente loi. Pour le solde des frais restant à couvrir dans le cadre de ses missions conférées par la présente loi, la Commission nationale bénéficiera d'une dotation d'un montant à déterminer sur une base annuelle et à inscrire au budget de l'Etat. »

Ainsi décidé à Esch-sur-Alzette en date du 20 février 2004

La Commission nationale pour la protection des données

(*s.*) Gérard Lommel	(*s.*) Edouard Delosch	(*s.*) Pierre Weimerskirch
Président	Membre effectif	Membre effectif

Avis du 20 février 2004 de la Commission nationale pour la protection des données relatif à l'avant-projet de règlement grand-ducal fixant les modalités ayant trait aux missions du chargé de la protection des données

Délibération n° 4/2004 du 20 février 2004

Les dispositions des articles 12 paragraphe 3 a) et 40 de la loi prévoient expressément la possibilité pour le responsable du traitement de désigner un chargé de la protection de données.

Toutefois les modalités de désignation et de révocation ainsi que l'exécution des missions du chargé de la protection des donnés, de même que ses relations avec la Commission nationale devront être fixées par règlement grand-ducal (article 40 paragraphe 10 de la loi).

Commentaires des articles de l'avant-projet propos

Préambule

Les particularités de la procédure de nomination du chargé de la protection des données se caractérisent par:

- l'agrément, respectivement le refus d'agrément
- la désignation de même que le refus de désignation (càd l'opposition)

(1) L'agrément

Les paragraphes 6 et 7 de l'article 40 prévoient expressément les conditions auxquelles l'agrément est subordonné, à savoir: la justification d'une formation universitaire en droit, économie, gestion d'entreprise, science de la nature ou informatique.

Par ailleurs la loi impose également l'assujettissement à des assises financières de € 20.000.

Le Commission nationale constate que la référence faite à la preuve de l'obtention d'un titre universitaire et d'une assise financière a été reprise de la loi du 31 mai 1999 régissant la domiciliation des sociétés1.

Le paragraphe 7 prévoit une exception quant à la nécessité de fournir des assises financières pour certaines catégories de professions bien déterminées et réglementées.

Il s'ensuit que dès qu'un chargé de la protection des données soumet une demande et ne remplit pas une des conditions2 prédéfinies supra, l'agrément lui est refusé.

(2) La désignation

La désignation est l'étape ultérieure dans le processus de nomination et présuppose péremptoirement que les conditions de l'agrément soient remplies.

D'après l'article 40 paragraphe 1er de la loi, il incombe au responsable du traitement de désigner un chargé de la protection des donnes dont il communique l'identité à la Commission nationale.

D'après l'article 3 du projet de règlement grand-ducal sous avis, le responsable du traitement désigne celui-ci sur base de la liste des chargés agréés.

D'après l'article 40 paragraphe 8, la Commission nationale vérifie les qualités de tout chargé de la protection des données. Elle peut s'opposer à tout moment à la désignation ou au maintien du chargé de la protection des données lorsqu'il ne présente pas (càd lorsque ces qualités font défaut ab initio) ou plus (càd lorsque les qualités dans le chef du chargé ne sont plus remplies postérieurement à sa désignation) les qualités requises pour la fonction en question ou lorsqu'il est déjà en relation avec le responsable du traitement et que cette relation fait naître un conflit d'intérêts limitant son indépendance.

[1] document parlementaire n°4735[00], page 51

[2] ou ne les remplit plus au moment où la Commission nationale prend sa décision

Le paragraphe 9 donne implicitement pouvoir à la Commission nationale de définir les modalités du contrôle continu des qualités requises à la fonction de chargé de la protection des données

A ce sujet la Commission nationale préconise d'instaurer des séances de formation continue auxquelles chaque chargé de la protection des données sera tenu d'assister deux fois par an ainsi que la participation à des séminaires d'information.

L'article 40 paragraphe 8 alinéa 2 dispose qu'« en cas d'opposition de la Commission nationale, le responsable du traitement dispose de 3 jours pour désigner un nouveau chargé de la protection des données ».

La Commission nationale s'interroge si en cas d'opposition un recours administratif est ouvert au chargé de la protection des données révoqué auquel la décision intervenue fait grief.

Par ailleurs ne conviendrait-il pas de préciser qu'à défaut de désignation d'un nouveau chargé de la protection des données dans le délai (de 3 jours) imparti par la loi, le responsable du traitement ne saurait plus bénéficier de l'exemption de l'obligation de notification prévue à l'article12 paragraphe (3) de la loi ?

Article 1

Cet article prévoit la possibilité de délivrer l'agrément sur contrôle des pièces. Il serait plus judicieux de rallonger le délai en cas de refus implicite à trois mois au lieu d'un mois en se conformant ainsi aux principes généraux applicables en droit administratif. En effet aucune disposition de même qu'aucune raison particulière tenant à l'urgence justifie le raccourcissement du délai.

Par ailleurs, la dernière phrase de l'avant-projet de règlement grand-ducal est à biffer dans la mesure où elle n'est qu'une application concrète de la procédure administrative non contentieuse.

Article 2

La Commission nationale constate que la deuxième phrase de l'article 2 relatif à l'honorabilité professionnelle n'est, entre autres, qu'une reprise textuelle de l'article 7 paragraphe 1 de la loi modifiée du 5 avril 1993 relative au secteur financier.

A ce sujet la Commission nationale aimerait préciser que la loi apporte une définition claire et précise s'agissant de l'agrément3. De même la loi donne implicitement compétence à la Commission nationale pour délimiter les contours relatifs aux « qualités requises » pour la fonction de chargé de la protection des données.

Toutefois à défaut de disposition légale afférente, la Commission nationale s'interroge comment pouvoir procéder en toute objectivité à la vérification de la notion d'« honorabilité professionnelle » dans le chef du chargé de la protection des données dans la mesure où la loi n'apporte guère de précisions complémentaires à ce sujet.

Si l'intention du législateur est celle de faire de cette notion une condition sine qua non de l'obtention de l'agrément, il doit en être tenu compte dans les amendements à apporter à la loi dans le projet de loi n°5181 alors qu'un règlement grand-ducal, portant exécution d'une loi, ne saurait ajouter des dispositions en sus à celle-ci.

Article 3

La Commission nationale suggère de rectifier le point a) de l'article 3 en précisant qu'«elle dresse et tient à jour une liste des chargés de la protection des données agréés au Luxembourg ».

L'article 12 paragraphe 3 a) dispose que le responsable du traitement peut désigner un chargé de la protection des données qui est tenu d'assurer de manière indépendante l'application des dispositions légales.

[3] formation universitaire et assises financières

L'article 40 paragraphe 8 b) dispose notamment que la Commission nationale peut s'opposer à la désignation ou au maintien du chargé de la protection des données si ce dernier est en relation4 avec le responsable du traitement et que cette relation fait naître un conflit d'intérêts limitant son indépendance.

Toutefois la Commission nationale constate que le secret professionnel énoncé à l'article 24 paragraphe 2 de la loi et relatif au chargé de la protection des données agissant dans le cadre de l'accomplissement de ses missions ne concerne que le secret professionnel visant les données traitées par ce dernier, secret qui n'est d'ailleurs pas opposable à la Commission nationale5.

Partant, il ne s'agit pas du secret professionnel en vertu duquel le chargé de la protection des données est tenu envers le responsable du traitement avec lequel il est « en relation »6.

Dès lors force est de constater que la Commission nationale ne dispose d'aucun moyen d'action concret afin de vérifier l'indépendance du chargé de la protection des données envers le responsable du traitement et dont il est question à l'article 40 paragraphes 3 et 8 b).

Article 4

La situation des avocats à la Cour étant claire, la Commission nationale part donc du principe que les avocats stagiaires (càd ceux de l'ancienne liste II) sont, en interprétant a contrario les termes du texte, soumis à la contrainte de produire des assises financières de € 20.000.

Mais quid des avocats de la liste IV, càd ceux pouvant exercer au Luxembourg la profession d'avocat sous leur titre d'origine ? Sont-ils astreints aux assises financières ou assimilés aux avocats à la Cour ?

S'agissant de ces assises financières, la Commission nationale s'interroge comment cette garantie doit-elle être concrètement mise en œuvre ?

Faut-il placer le montant en question sur un compte bloqué, disposer d'une infrastructure locale suffisante7 ou fournir caution ? Est-ce que le fait de souscrire une police d'assurance spéciale ou détenir des valeurs mobilières correspondant au montant en question respectent l'exigence du texte ?

Il faudrait donc impérativement régler ces détails par voie de règlement grand-ducal.

L'article 40 paragraphe 5 de la loi précise que peuvent être désignés à la fonction de chargé de la protection des données des personnes physiques ou morales.

S'agissant des personnes morales, la Commission nationale estime qu'il faudrait indiquer de façon claire et sans équivoque quelle personne physique déterminée au sein de ce groupement est susceptible d'agir en tant que chargé de la protection des données.

La Commission nationale suggère de préciser que cette personne physique représentant l'être moral n'aurait pas la faculté de déléguer son pouvoir (pouvoir de délégation et/ou pouvoir de signature, voire pouvoir de substitution).

Dans le même ordre d'idées, la Commission nationale estime que seule la personne physique au sein de l'être moral et remplissant les conditions d'agrément et de désignation devrait être qualifiée de chargé de la protection des données. Toute autre personne salariée de la personne morale ne peut accomplir une mission pour compte du chargé de la protection des données.

---

[4] la Commission nationale souligne que le législateur n'apporte aucune précision complémentaire quant à cette notion de « *relation* ». Faute de précision textuelle, on peut admettre qu'il s'agisse *lato sensu* de relations d'affaires **ponctuelles** ou **continues** entre le chargé de la protection des données et le responsable du traitement

[5] article précité

[6] *i.e.*: le secret professionnel liant l'avocat à son client, le secret médical…

[7] bureau, mobilier….

Finalement l'article 4 point a) du projet de règlement grand-ducal est à biffer[8] dans la mesure où la loi n'opère pas la distinction à laquelle aboutira ledit texte réglementaire.

La loi prévoit uniquement le cas de désigner un chargé de la protection des données. Reste ouverte la question si un responsable du traitement peut désigner 2 ou plusieurs chargés de la protection des données. La Commission nationale estime que tel devrait être le cas.

Article 5

La Commission nationale approuve la disposition imposant au chargé de la protection des données de communiquer le relevé des traitements nouveaux tous les quatre mois.

Il serait en outre judicieux d'indiquer quelles mentions ce relevé devrait comporter.

La Commission nationale estime que, par analogie avec la notification effectuée par le responsable du traitement, le relevé dont question devrait comporter au moins les mentions figurant à l'article 13 de la loi.

Au vœu de l'article 22 de la loi, le responsable du traitement est tenu d'établir un rapport annuel relatif aux mesures techniques et d'organisation prises pour assurer la sécurité des traitements.

Si toutefois le responsable du traitement désigne un chargé de la protection des données, la Commission nationale considère qu'il serait dans la logique du texte de prévoir que l'établissement de ce rapport annuel confié au responsable du traitement devrait être avisé par le chargé de la protection des données assurant sa transmission à la Commission nationale.

Article 6

La Commission nationale ne saurait partager l'approche de l'avant-projet de règlement grand-ducal consistant à prévoir que les traitements effectués pendant la période de vacation continuent à être régis par l'article 40 de la loi pendant un délai d'un mois.

Elle estime que le droit commun visé aux articles 12 et 13 de la loi devrait s'appliquer en pareil cas, une telle période de vacation n'étant pas prévue par la loi.

L'article 40 paragraphe 10 de la loi prévoit expressément que les modalités de désignation et de révocation du chargé de la protection des données seront fixées par règlement grand-ducal.

L'avant-projet de règlement grand-ducal proposé ne prévoit ni les modalités concrètes de révocation du chargé de la protection des données[9] ni celles de sa désignation.

Le projet en question reste aussi muet sur les modalités d'exécution des missions du chargé de la protection des données de même que des relations entre ce dernier avec la Commission nationale.

Article 7

Cet article n'appelle pas d'observations particulières de la part de la Commission nationale.

Ainsi décidé à Esch-sur-Alzette en date du 20 février 2004

La Commission nationale pour la protection des données

(*s.*)Gérard Lommel	(*s.*)Edouard Delosch	(*s.*)Pierre Weimerskirch
Président	Membre effectif	Membre effectif

[8] d'après l'adage : « *ubi lex non distinguit nec nos distinguere debemus* »
[9] *i.e.*: nécessité de procéder à révocation par envoi de lettre recommandée, l'obligation pour le responsable du traitement d'indiquer le motif justifiant, d'après lui, la fin des relations avec le chargé de la protection des données donnerait la possibilité au juge de vérifier, en cas de saisine de celui-ci, le garde-fou figurant à l'article 40 paragraphe 3 b)

Avis de la Commission nationale pour la protection des données concernant la loi du 6 juillet 2004 modifiant la loi du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques

Délibération n°74/2004 du 13 septembre 2004

Suite à la demande lui adressée par courrier du 4 mars 2004 de Monsieur le Ministre des Transports, la Commission nationale entend présenter ci-après ses observations et commentaires au sujet du projet de loi n°5256 modifiant la loi du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques, bien que ce projet de loi vienne d'être définitivement adopté entre-temps par la loi du 6 juillet 2004 (publiée au Mémorial A, n° 134 du 28 juillet 2004).

A) L'article 4 bis paragraphe 4 de la loi du 6 juillet 2004 modifiant la loi du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques

Dans son courrier adressé à la Commission nationale, Monsieur le Ministre des Transports demande l'avis de celle-ci sur le point de savoir si le texte proposé au niveau de cet article, qui soulève une question en termes de protection des données, est « suffisant pour constituer la base légale requise ».

Le libellé de l'article en question se présente comme suit :

« Le Ministre des Transports peut confier à la Société Nationale de Contrôle Technique des tâches administratives relevant de la gestion de l'immatriculation des véhicules routiers et de la gestion des permis de conduire. La mise en œuvre de cette gestion peut être déterminée par un règlement grand-ducal.

Sans préjudice des dispositions de la législation relative à la protection des personnes à l'égard du traitement des données à caractère personnel, le Ministre des Transports est autorisé, dans le cadre de la gestion des permis de conduire, à collecter, utiliser et traiter des données relatives à la santé et des données judiciaires. Cette même autorisation vaut pour la Société Nationale de Contrôle Technique, agissant comme sous-traitant du Ministre des Transports dans l'accomplissement de ses missions légales prévues au premier alinéa du présent paragraphe.

Les employés de la Société Nationale de Contrôle Technique qui sont chargés de la réception des examens en vue de l'obtention d'un permis de conduire sont agréés par le Ministre des Transports. Avant d'entrer en fonction, les agents affectés à la réception des examens du permis de conduire prêteront devant le Ministre des Transports ou son délégué le serment qui suit: «Je jure de remplir mes fonctions avec intégrité, exactitude et impartialité.»

B) Les travaux parlementaires relatifs au projet de loi n° 5256

Les seuls développements se rapportant à l'article en question dans les travaux parlementaires sont les suivants :

« Il est proposé de profiter du projet de loi en question pour introduire une base légale permettant le traitement des données relatives aux décisions judiciaires et des données médicales en relation avec la gestion du permis de conduire par les services du Ministère des Transports et ceux de la Société Nationale de Contrôle Technique à laquelle cette gestion a été déléguée pour partie en vertu de la loi du 30 juillet 2002. Aux termes de la législation sur la protection des données à caractère personnel la Société Nationale de Contrôle Technique fait fonction de sous-traitant vis-à-vis du Ministère des Transports. » (cf. document parlementaire n°5256/00, exposé des motifs, p. 9 et 10).

Par la loi du 30 juillet 2002 le Ministre des Transports a été autorisé à confier à la Société Nationale de Contrôle Technique (SNCT) des tâches administratives relevant de la gestion des permis de conduire. Tant pour le Ministère des Transports que pour la SNCT en vertu de la délégation précitée la gestion du permis de conduire requiert le traitement des données médicales et des données judiciaires.

Comme ces données subissent un traitement, elles tombent sous le champ d'application des dispositions de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et le traitement nécessite une autorisation légale. Le deuxième alinéa du quatrième paragraphe de l'article 4bis propose d'introduire une base légale permettant le traitement de ces données par le Ministre des Transports et la SNCT en tant que sous-traitant. (cf. document parlementaire n°5256/00, commentaire des articles, p. 16).

« IV. La base légale relative au traitement des données

Suivant les explications des auteurs du projet de loi, il est introduit une base légale permettant le traitement de données relatives aux décisions judiciaires et des données médicales en relation avec la gestion du permis de conduire par les services du Ministère des Transports et ceux de la Société Nationale du Contrôle Technique à laquelle cette gestion a été déléguée pour partie en vertu de la loi du 30 juillet 2002. Afin de suffire aux dispositions de la loi sur la protection des données à caractère personnel, il est expressément précisé que la Société Nationale de Contrôle Technique mandatée de par la loi à concourir à côté du Ministère des Transports à la gestion administrative des immatriculations automobiles et des permis de conduire (est appelée) à faire fonction de sous-traitant du Ministère des Transports dans le cadre du traitement des données personnelles susceptibles d'être utilisées dans le cadre des missions précitées » (cf. document parlementaire n°5256/04, RAPPORT DE LA COMMISSION DE L'ECONOMIE, DE L'ENERGIE, DES POSTES ET DES TRANSPORTS, p. 16).

C) La directive 95/46/CE du 24 octobre 1995

1) La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données prévoit en ses considérants 53 et 54 :

« (53) considérant que, cependant, certains traitements sont susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées, du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, ou du fait de l'usage particulier d'une technologie nouvelle; qu'il appartient aux États membres, s'ils le souhaitent, de préciser dans leur législation de tels risques;

(54) considérant que, au regard de tous les traitements mis en oeuvre dans la société, le nombre de ceux présentant de tels risques particuliers devrait être très restreint; que les États membres doivent prévoir, pour ces traitements, un examen préalable à leur mise en oeuvre, effectué par l'autorité de contrôle ou par le détaché à la protection des données en coopération avec celle-ci; que, à la suite de cet examen préalable, l'autorité de contrôle peut, selon le droit national dont elle relève, émettre un avis ou autoriser le traitement des données; qu'un tel examen peut également être effectué au cours de l'élaboration soit d'une mesure législative du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et précise les garanties appropriées ».

2) La directive 95/46/CE prévoit à l'article 20 intitulé « Contrôles préalables » que

« 1. Les États membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en œuvre.

2. De tels examens préalables sont effectués par l'autorité de contrôle après réception de la notification du responsable du traitement ou par le détaché à la protection des données, qui, en cas de doute, doit consulter l'autorité de contrôle.

3. Les États membres peuvent aussi procéder à un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées. »

D) Observations de la Commission nationale pour la protection des données

Aux termes des travaux parlementaires relatifs au projet de loi n°4735 ayant conduit à la loi du 2 août 2002, il appert que la volonté du législateur était celle de créer au Grand-Duché de Luxembourg une loi-cadre en matière de protection des données :

« II.3. Une loi cadre

a) Un cadre de la loi dessiné en forme de balance

La directive, et plus particulièrement encore le présent projet de loi, sont des instruments encadrant l'ensemble des activités humaines liées aux données personnelles. Il s'agit donc d'un cadre extrêmement vaste, dans lequel s'insère un certain nombre de législations spéciales comme la législation sur les établissements hospitaliers ou encore la législation sur le commerce électronique et plus particulièrement les dispositions relatives à la signature électronique.

Ce cadre dessine l'articulation des différents textes qui interviennent sectoriellement ainsi que l'articulation des principes fondateurs de la Directive 95/46/CE avec les situations particulières exigeant des adaptations. Il s'agit donc de faire la balance des intérêts en présence. » (cf. document parlementaire n°4735/00, p. 84).

La Commission nationale constate que le traitement autorisé de par la loi du 6 juillet 2004 concerne à la fois des données judiciaires régies par l'article 8 de la loi du 2 août 2002 et des données relatives à la santé visées aux articles 6 et 7 de la même loi.

Or c'était un choix délibéré et judicieux du législateur d'instaurer une loi-cadre qui régisse de manière exhaustive la matière de la protection des données personnelles.

Force est de constater que la loi du 2 août 2002 ne prévoit pas la possibilité d'une autorisation par voie légale des traitements de données relatives à la santé, mais seulement l'autorisation par la Commission nationale. La disposition sous avis s'écarte donc d'une option privilégiant l'unité et la lisibilité du cadre légal, ce qui paraît regrettable.

1) Données judiciaires

Suivant l'article 8 paragraphe 5 de la directive 95/46/CE, « le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'Etat membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique. »

En vertu de l'article 8 paragraphe 2 de la loi du 2 août 2002, « le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être mis en œuvre qu'en exécution d'une disposition légale. »

C'est en application de l'article 8, paragraphe 2 précité que le législateur a introduit une base légale spécifique nouvelle permettant le traitement des données relatives aux décisions judiciaires en relation avec la gestion des permis de conduire.

Cette autorisation par voie légale du traitement des données judiciaires est conforme à l'esprit de la loi du 2 août 2002 qui ne donne pas compétence à la Commission nationale pour autoriser une telle catégorie particulière de données (voir en ce sens l'article 14 paragraphe 1er de la loi).

En règle générale, cet examen préalable incombe à la Commission nationale et aboutit à une autorisation (ou refus) motivé(e) à la suite d'une analyse concrète du traitement envisagé (décrit dans la demande introduite par le responsable du traitement) sous l'angle de tous les principes (en l'occurrence les principes de transparence, de finalité, de nécessité, de proportionnalité et d'exactitude) prévus à l'article 4 paragraphe 1er de la loi du 2 août 2002 aux termes duquel :

« Le responsable du traitement doit s'assurer que les données qu'il traite le sont loyalement et licitement, et notamment que ces données sont:

(a) collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités;

(b) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;

(c) exactes et, si nécessaire, mises à jour; toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;

(d) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées… ».

Il revient également à la Commission nationale de vérifier si la confidentialité et la sécurité des données sont assurées et au besoin d'imposer des conditions ou restrictions à respecter lors de la mise en œuvre.

Force est de constater que la Chambre des Députés n'a pas défini les caractéristiques exactes du traitement autorisé, ni précisé les données ou catégories de données judiciaires qui font l'objet du traitement opéré par le Ministère des Transports (et par la SNCT), ni fixé des garanties appropriées au regard des droits et libertés des personnes concernées.

De plus, la loi du 6 juillet 2004 ne contient aucune disposition sur les garanties appropriées, à moins que l'on puisse dire que ces garanties seront réglées selon les dispositions générales édictées à la loi du 2 août 2002, et plus particulièrement aux articles 21 à 25.

2) Données relatives à la santé

Quant au traitement des données médicales, le législateur a choisi une voie originale pour autoriser ce type de traitement en adoptant la loi du 6 juillet 2004 qui s'écarte comme il a été relevé ci-avant de la logique de la loi-cadre du 2 août 2002.

En effet, tout en rappelant que les dispositions de la loi du 2 août 2002 sont pleinement applicables au traitement envisagé, la loi du 6 juillet 2004 y déroge en autorisant légalement le traitement de données relatives à la santé, alors qu'au regard des articles 6 et 7 (combinés à l'article 14 paragraphe 1er) de la loi du 2 août 2002 une autorisation préalable de la part de la Commission nationale est en principe requise.

S'il est vrai que cette façon d'agir n'est pas contraire en tant que telle à la directive 95/46/CE, puisque l'article 20 paragraphe 3 de la directive 95/46/CE prévoit expressément que « les États membres peuvent aussi procéder à un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées », il n'en demeure pas moins que la Commission nationale se doit de relever que les dispositions de l'article 20 de la directive 95/46/CE n'ont pas été respectées par le législateur luxembourgeois lors de l'adoption de l'article 4 bis paragraphe 4 de la nouvelle du 6 juillet 2004, étant donné qu'il ne résulte aucunement des travaux parlementaires que le législateur a procédé au examen préalable exigé par l'article 20 de la directive.

En outre, il n'a ni défini les caractéristiques exactes du traitement autorisé, ni fixé des garanties appropriées au regard des droits et libertés des personnes concernées.

Conclusion ad) points 1) et 2) de la rubrique D)

Au stade actuel, la Commission nationale considère dès lors que la directive 95/46/CE n'a pas été respectée dans la mesure où le législateur n'a pas encore procédé à l'examen de proportionnalité, tel que prescrit par l'article 20 de la directive.

En effet, il ne résulte aucunement des travaux parlementaires qu'une discussion afférente a été menée par les différents intervenants au cours de la procédure législative, et plus précisément lors de l'élaboration de l'article 4 bis paragraphe 4 de la nouvelle loi du 6 juillet 2004.

Cependant, compte tenu de la marge de manoeuvre laissée aux Etats-membres par l'article 20 de la directive 95/46/CE qui permet en quelque sorte de reporter cet examen de proportionnalité jusqu'à l'élaboration d'une mesure fondée sur une mesure législative, le Grand-Duché de Luxembourg devra au plus tard lors de l'adoption du règlement grand-ducal, pris en exécution de la loi du 6 juillet 2004, procéder à l'examen prescrit par la directive en définissant la nature du traitement et en fixant des garanties appropriées.

Il semble d'ailleurs que la volonté du législateur de procéder à un tel examen ultérieur se retrouve au niveau du premier alinéa de l'article 4 bis paragraphe 4 de la loi du 6 juillet 2004 qui prévoit expressément que la mise en œuvre de la gestion des permis de conduire « peut être déterminée par un règlement grand-ducal », avec la restriction que le texte légal aurait dû employer le terme « doit » au lieu de « peut » pour être tout à fait conforme à la directive.

A l'occasion de l'élaboration dudit projet de règlement grand-ducal, la Commission nationale devra être utilement demandée en son avis afin de préciser les conditions de licéité dudit traitement, et ceci conformément à l'article 32 paragraphe 3, lettre (e) de la loi du 2 août 2002 aux termes duquel la Commission nationale pour la protection des données a pour mission d'« être demandée en son avis sur 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 ».

3) Considérations additionnelles

Finalement la Commission nationale aimerait attirer l'attention sur le caractère hautement sensible des données traitées par la Société Nationale de Contrôle Technique (SNCT), agissant en qualité de sous-traitant, pour compte du Ministère des Transports.

a) En vertu du règlement ministériel du 10 mars 1983 fixant les modalités du certificat médical pour l´obtention d´un permis de conduire, le certificat médical pour l´obtention et le renouvellement d´un permis de conduire portera, outre le résultat proprement dit de l'examen médical, sur un questionnaire qui est à remplir par le médecin-examinateur libellé comme suit :

1. Antécédents de l´examiné

- maladies,
- opérations,
- accidents.

2. L´examiné a-t-il été atteint de

a) maladies cardiaques,

b) diabète,

c) maladies du sang,

d) déficience rénale grave,

e) maladies du système nerveux,

f) vertiges, syncopes ou malaises analogues,

g) crises convulsives ou crises équivalentes,

h) traumatisme crânio-cérébral,

i) l´examiné a-t-il commis des abus de soporifiques, de stupéfiants, ou de boissons éthyliques?

j) l´examiné a-t-il subi une cure (de désintoxination ou autre) dans un établissement psychiatrique?

b) De même, l'arrêté grand-ducal du 23 novembre 1955 portant règlement de la circulation sur toutes les voies publiques, tel que modifié par la suite, prévoit notamment que

« C. – Les conditions médicales à remplir par les conducteurs

Art. 77. En vue de l'obtention ou du renouvellement d'un permis de conduire, l'intéressé doit se soumettre à un examen médical destiné à établir s'il ne souffre pas d'infirmités ou de troubles susceptibles d'entraver ses aptitudes ou capacités de conduire et s'il ne présente pas de signes d'alcoolisme ou d'autres intoxications. Sur avis de la commission médicale prévue à l'article 90, le titulaire d'un permis de conduire peut de même être obligé par le ministre des Transports à se soumettre à un examen médical, s'il existe des doutes sur ses aptitudes ou capacités de conduire.

L'examen médical porte notamment sur la capacité visuelle, l'audition, les affections cardiovasculaires, les troubles endocriniens, les maladies du système nerveux, les troubles mentaux, l'alcoolisme, la consommation de drogues et de médicaments, les maladies du sang et les maladies de l'appareil génito-urinaire ainsi que sur l'état de santé général et les incapacités physiques. »

S'agissant de données sensibles, la Commission nationale rappelle que la confidentialité de ces données doit être garantie tant par le responsable du traitement que par le sous-traitant au regard des dispositions des articles 22 et 23 de la loi du 2 août 2002.

« L'ensemble des mesures de sécurité doit conférer un „niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger" (cf. document parlementaire 4735/13 p.37 et Directive 95/46/CE, article 17, paragraphe 2).

Ces mesures doivent également viser à prévenir tout autre risque d'atteinte aux données tel que leur vol, leur effacement, etc., ainsi que tout risque d'utilisation pour d'autres finalités (cf. avis d'initiative relatif aux traitements d'images effectués en particulier par le biais de systèmes de vidéosurveillance, n° de rôle 34/99 du 13/12/1999 (Commission pour le protection de la vie privée, Belgique)).

En l'espèce, des mesures de sécurité particulières, telles que prescrites aux articles 22 et 23 de la loi du 2 août 2002, s'imposent.

Vu le caractère délicat des données traitées, il faut s'interroger sur l'opportunité, voire la nécessité de sous-traiter une telle activité à une société de droit privé (en l'occurrence une société à responsabilité limitée), en dépit du fait que la loi du 30 juillet 2002 (repris à l'article 4bis paragraphe 4 de la loi du 6 juillet 2004) a autorisé le Ministre des Transports à confier à la Société Nationale de Contrôle Technique (SNCT) des tâches administratives relevant de la gestion des permis de conduire.

On peut même se demander si les employés de cette société sont suffisamment qualifiés pour apprécier les renseignements médicaux fournis et si ces données ne devraient pas être conservées sous le couvert du secret médical.

En effet, contrairement à la commission médicale instituée par l'article 90 de l'arrêté grand-ducal du 23 novembre 1955 précité en vue d'examiner les personnes souffrant d'infirmités ou de troubles susceptibles d'entraver leurs aptitudes ou capacités de conduire un véhicule automoteur ou cyclomoteur, les employés de la SNCT ne sont pas soumis au respect du secret médical prévu à l'article 458 du code pénal.

Il est vrai que suivant l'article 4bis paragraphe 4 dernier alinéa de la loi du 6 juillet 2004 les employés de la Société Nationale de Contrôle Technique, qui sont chargés de la réception des examens en vue de l'obtention d'un permis de conduire, sont agréés par le Ministre des Transports et prêtent devant le Ministre des Transports ou son délégué le serment qui suit: « Je jure de remplir mes fonctions avec intégrité, exactitude et impartialité ». Le projet de loi est toutefois muet sur la portée d'un tel agrément et d'une telle assermentation. L'employé de la SNCT agréé et assermenté peut-il être assimilé pour autant à une personne soumise à un secret professionnel ?

Dans la mesure où la gestion du permis de conduire requiert le traitement des données médicales et des données judiciaires dans le chef du Ministère des Transports en sa qualité de responsable du traitement, il est important en outre que l'étendue de la mission confiée en la matière au sous-traitant SNCT soit précisé et documentée conformément à l'article 22 paragraphe 3 de la loi du 2 août 2002.

Ainsi décidé à Esch-sur-Alzette en date du 13 septembre 2004.

Pour la Commission nationale pour la protection des données

(*s.*) Gérard Lommel	(*s.*) Edouard Delosch	(*s.*) Pierre Weimerskirch
Président	Membre effectif	Membre effectif

Délibération n°76/2004 du 17 septembre 2004 de la Commission nationale pour la protection des données relative au sujet de la demande du Fonds de garantie automobile à la direction générale de la police grand-ducale

Conformément à l'article 32, paragraphe 3, lettre (e) de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, la Commission nationale pour la protection des données a entre autres pour mission d'« être demandée en son avis sur 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, et faisant suite à la demande lui adressée par courrier du 23 mars 2004 de Monsieur le Directeur Général de la Police grand-ducale, que la Commission nationale entend présenter ci-après plusieurs observations sur les dispositions légales et réglementaires lui soumises pour avis.

A) Le contexte légal et réglementaire applicable

En premier lieu, le Directeur Général de la police grand-ducale s'interroge sur la légalité de la transmission des procès-verbaux et rapports de la police grand-ducale au Fonds de garantie automobile, au motif que la procédure prévue à l'article 22 de la loi du 16 avril 2003 relative à l'assurance obligatoire de la responsabilité civile en matière de véhicules automoteurs fait intervenir le Ministère Public, tandis que l'article 18 du règlement grand-ducal du 11 novembre 2003 pris en exécution de la loi du 16 avril 2003 fait état de la police grand-ducale.

1) La loi du 16 avril 2003

La loi du 16 avril 2003 relative à l'assurance obligatoire de la responsabilité civile en matière de véhicules automoteurs prévoit à l'article 22 :

« 1. Tout sinistre devant donner lieu à l'intervention du Fonds conformément aux points 1, 2, 3 et 4 de l'article 16 de la présente loi doit lui être dénoncé dans les six mois, à peine de forclusion, à moins que la personne lésée ne prouve qu'elle a été dans l'impossibilité physique ou morale de faire cette dénonciation dans le délai prescrit.

2. Toute action récursoire du Fonds sera prescrite après trois ans à compter du règlement effectué par le Fonds en conformité des dispositions de la présente loi.

3. Dans les affaires portées devant les juridictions répressives, le ministère public est tenu d'informer le Fonds de l'ouverture de l'instruction, de l'inviter à prendre inspection des dossiers dès la clôture de l'instruction et de lui faire tenir une copie de la citation à l'audience notifiée aux prévenus ».

Les travaux parlementaires prévoient dans ce contexte que :

« L'article 22 reprend les dispositions de l'article 7 de la loi du 16 décembre 1963. Le point 1 impose à toute personne lésée d'adresser, sous peine de forclusion, sa demande d'indemnisation au Fonds endéans un délai de 6 mois à compter de la date de la survenance du sinistre à moins qu'elle puisse prouver qu'elle était dans l'impossibilité de le faire.

Le point 2 prévoit que toute action récursoire du Fonds se prescrit après trois ans.

Le point 3 oblige le ministère public d'informer le Fonds sur les affaires portées devant les juridictions répressives. » (cf. document parlementaire n°5030/00, p. 21).

2) Le règlement grand-ducal du 11 novembre 2003

Le règlement grand-ducal du 11 novembre 2003 relatif au fonctionnement du Fonds de garantie automobile (pris en exécution de la loi du 16 avril 2003 précité) prévoit à l'article 18 :

« La police grand-ducale transmet au Fonds dans les dix jours de la clôture un exemplaire de tout procès-verbal ou rapport relatif à un accident ayant été causé sur le territoire du Grand-Duché de Luxembourg par un véhicule inconnu ou non assuré. »

Comme le relève à juste titre le Directeur Général de la police grand-ducale, la Commission nationale estime que la procédure instaurée par l'article 22 de la loi du 16 avril 2003 diffère de celle décrite à l'article 18 du règlement grand-ducal du 11 novembre 2003.

En effet, l'article 22 de la loi du 16 avril 2003 prévoit en son premier paragraphe qu'il incombe à la personne lésée de faire la dénonciation du sinistre endéans les six mois au Fonds de Garantie Automobile. Par ailleurs, le troisième paragraphe du même article mentionne que dans les affaires pénales le Ministère Public doit lui faire tenir une copie de la citation à l'audience notifiée aux prévenus.

Force est de constater que l'article 22 de la loi du 16 avril 2003 ne fait donc nullement intervenir la police grand-ducale. Ce n'est que l'article 18 du règlement grand-ducal du 11 novembre 2003 qui fait intervenir un nouvel acteur, à savoir la police grand-ducale.

Comment la situation était-elle réglée sous l'empire de la loi antérieure ?

La teneur de l'article 7, paragraphe 3, de la loi abrogée du 16 décembre 1963 portant création d'un Fonds commun de garantie automobile était la suivante :

« Dans les affaires portées devant les juridictions répressives, les officiers du ministère public seront tenus d'informer le Fonds de l'ouverture de l'instruction, de l'inviter à prendre inspection des dossiers dès la clôture de l'instruction et de lui notifier une copie de la situation à l'audience délivrée aux prévenus. »

L'article 5 du règlement grand-ducal du 20 décembre 1991 portant modification du règlement grand-ducal du 9 juin 1964 pris en exécution de la loi du 16 décembre 1963 portant création d'un Fonds commun de garantie automobile prévoit que l'article 16 du règlement du 9 juin 1964 est modifié comme suit :

« Les autorités de la police ou de la gendarmerie doivent transmettre au Fonds dans les dix jours de la clôture un exemplaire de tout procès-verbal ou rapport relatif à un accident ayant été causé par un auteur inconnu ou non assuré.»

Il s'ensuit que le régime légal antérieur était quasiment identique au cadre légal actuel qui suscite des interrogations de la part de la direction générale de la police.

En dépit du fait que la législation antérieure contenait déjà des dispositions similaires, il n'en reste pas moins qu'il est permis de se demander, comme le fait la direction générale de la police, si le règlement grand-ducal du 11 novembre 2003 n'est pas contraire sur ce point à la loi du 16 avril 2003, voire va même au-delà du cadre légal tracé.

B) La transmission des procès-verbaux et rapports de la police grand-ducale au Fonds de garantie automobile équivaut-elle à une interconnexion au sens de l'article 16 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ?

Dans son courrier du 23 mars 2004, le Directeur Général de la police grand-ducale aimerait en outre avoir « de plus amples directives quant à la procédure à suivre, eu égard notamment à l'article 16 de la loi du 2 août 2002, avant de faire droit à la demande du Fonds d'une transmission systématique et automatique ».

La Commission nationale en déduit que la police grand-ducale se demande si la transmission des procès-verbaux et rapports de la police grand-ducale au Fonds de garantie automobile équivaut à une interconnexion de données au sens de l'article 16 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ?

1) L'interconnexion de données

L'article 2, lettre (j), de la loi définit l' "interconnexion" comme étant « toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d'autres responsables du traitement ».

Est-ce que l'on est en présence d'une interconnexion de données au sens de l'art. 16 de la loi dans le cas de traitements opérés par un seul responsable du traitement ?

S'il est vrai que dans le projet de loi initial (cf. document parlementaire n°4735/00, page 2), l'interconnexion était définie comme étant "toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour une autre finalité par le même responsable du traitement ou par un ou d'autres responsables du traitement", il n'en reste pas moins que la Commission des Médias et des Communications a adopté le 4 juillet 2002 un amendement au sujet de la notion d'interconnexion (cf. document parlementaire n°4735/11, page 2) en la redéfinissant comme étant "toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d'autres responsables du traitement".

C'est cette définition qui a été retenue en définitive par le législateur.

A la lecture du commentaire dudit document parlementaire, il appert qu' "il s'agit d'une part d'assurer la consistance avec l'article 16 (3) qui vise des finalités identiques ou liées. D'autre part, comme la demande d'interconnexion doit émaner conjointement de plusieurs responsables de traitement, la référence à l'article 2 (j) „au même responsable du traitement" a été supprimée. En effet, en cas de traitements ayant des finalités liées ou identiques effectués par un seul responsable du traitement, une notification unique ou une autorisation unique sont déjà prévues."

Il s'ensuit que l'on ne saurait parler d'interconnexion de données au niveau d'un seul et même responsable du traitement, alors qu'il convient de lire la définition visée sous l'article 2 lettre (j) comme étant « toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par "un autre ou plusieurs autres" responsables du traitement. »

Au vu des éléments fournis, la Commission nationale estime que la transmission des procès-verbaux et rapports de la police grand-ducale au Fonds de garantie automobile ne constitue pas une interconnexion au sens de la loi du 2 août 2002, étant donné que la police grand-ducale n'entend pas mettre en corrélation des données qu'elle traite avec des données traitées par le Fonds de garantie automobile.

En raison de la définition restrictive retenue par le législateur pour l'interconnexion de données qui vise toujours la mise en corrélation de données entre plusieurs responsables des traitements (et non comme en l'espèce pour un seul et même responsable du traitement), la communication à un destinataire (en l'occurrence le Fonds de garantie automobile) ne pourra être assimilée à une interconnexion au sens de la loi du 2 août 2002, bien qu'en règle générale la communication à un destinataire entraîne le plus souvent la corrélation des données qu'il traite d'ores et déjà avec celles qu'il reçoit en communication.

2) La communication des données à un destinataire

Comme dit ci-avant, le Fonds de garantie automobile est à considérer comme simple destinataire qui, en vue de l'accomplissement de sa mission légale lui conférée par les articles 16 et suivants de la loi précitée du 16 avril 2003, ne fait que recevoir communication des données en cause.

La notion de "destinataire" est définie à l'article 2 lettre d) de la loi du 2 août 2002 comme étant « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers ».

A ce stade, on peut s'interroger dans quelle mesure un tiers, c'est-à-dire, selon l'article 2 lettre r) de la loi du 2 août 2002 : « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placés sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilités à traiter les données (…) », a vocation à recevoir communication de données.

a) La condition de légitimité

Les bases légales permettant à un tiers de traiter des données issues de l'article 5 (1) b) et d) de la loi du 2 août 2002 sont les suivantes :

- lorsque « le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées » ;
- lorsque « le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er (…) ».

En l'occurrence, la mission d'intérêt public, sinon l'intérêt légitime, du « Fonds de garantie automobile » est une base légale pouvant légitimer la communication des données à ce tiers.

b) Le principe de finalité et la compatibilité des finalités

Un destinataire interne ne peut recevoir communication des données que dans le cadre de la réalisation de la finalité du responsable du traitement et ne doit pas exploiter ces données à d'autres fins. En d'autres termes, le destinataire interne n'a pas de finalité autre que celle de servir la réalisation de la finalité définie par le responsable du traitement sinon il est à considérer comme destinataire externe encore appelé « tiers ».

Quant au Fonds de garantie automobile qui est un tiers (destinataire externe), il va sans dire que la ou les finalités d'un traitement ne peuvent conduire à lui communiquer des données sans risquer de diluer complètement le principe de finalité lui-même.

Un tiers n'est tiers que vis-à-vis du responsable du traitement lui communiquant les données. Il est aussi, comme sujet de droits et d'obligations, un responsable du traitement des données qu'il s'est vu communiquer. S'il peut avoir une légitimité à se voir communiquer des données c'est comme responsable de traitement qu'il doit les recevoir.

La nature du traitement mis en œuvre par le tiers dépend des données communiquées et des finalités propres au tiers. On retrouve ici, les questions classiques que tout responsable de traitement doit se poser.

Conformément à l'article 4 paragraphe 1er lettre a) de la loi du 2 août 2002 qui dispose que les données traitées doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités », reste à examiner la compatibilité de cette communication de données à ce tiers, le respect de la finalité étant le principe de base à respecter.

Or la réponse est fournie par la loi elle-même en prescrivant expressément une telle communication de données.

En effet, une finalité compatible peut être définie comme une finalité que l'intéressé – à savoir la personne concernée - peut raisonnablement prévoir compte tenu de tous les facteurs pertinents ou qu'une disposition légale considère comme compatible.

« L'article 4, paragraphe 1er, de la loi belge du 11 décembre 1998 précise que la compatibilité doit tenir compte „notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables". La doctrine a critiqué une compatibilité automatique en cas de changement de finalité dû à une modification légale ou réglementaire. Le présent projet de loi ne saurait être interprété comme permettant une telle compatibilité automatique en cas de changement de l'environnement légal ou réglementaire. Cependant il ne saurait être exclu que, dans une situation particulière, un tel changement puisse être considéré comme compatible avec la finalité initiale, sans qu'il y ait automatisme » (cf. document parlementaire 4735/13, p. 10).

C) La nature des données à caractère personnel fournies au Fonds de garantie automobile

Avant d'aborder la problématique proprement dite, il paraît indiqué de rappeler l'article 8 paragraphe 5 de la directive 95/46/CE aux termes duquel :

« Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'Etat membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique. Les Etats membres peuvent prévoir que les données relatives aux sanctions administratives ou aux jugements civils sont également traitées sous le contrôle de l'autorité publique. »

En l'espèce, le périmètre des données à caractère personnel, respectivement leur nature, diffère en fonction de l'autorité publique qui est censée fournir des informations au Fonds de garantie automobile.

Les données personnelles qui peuvent être consultées par le Fonds de garantie automobile en vertu de l'article 22, paragraphe 3, de la loi du 16 avril 2003 constituent indubitablement des données judiciaires au sens de l'article 8 paragraphe 2 de la loi du 2 août 2002, qui dispose que le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être mis en œuvre qu'en exécution d'une disposition légale, de sorte qu'une base réglementaire ne saurait être à elle seule suffisante.

En revanche, les données personnelles communiquées au Fonds, à travers la transmission des procès-verbaux ou rapports par la police grand-ducale, sur base de l'article 18 du règlement grand-ducal du 11 novembre 2003 tombent en outre sous le coup de l'article 17 de la loi du 2 août 2002.

L'article 17 paragraphe 1er lettre a) de la loi du 2 août 2002 prévoit qu'une autorisation par voie réglementaire est nécessaire pour les traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions pénales qui sont réservés, conformément à leurs missions légales et réglementaires respectives, aux organes du corps de la police grand-ducale, de l'Inspection générale de la police et de l'administration des douanes et accises. Le règlement grand-ducal déterminera le responsable du traitement, la condition de légitimité du traitement, la ou les finalités du traitement, la ou les catégories de personnes concernées et les données ou les catégories de données s'y rapportant, l'origine de ces données, les tiers ou les catégories de tiers auxquels ces données peuvent être communiquées et les mesures à prendre pour assurer la sécurité du traitement en application de l'article 22 de la présente loi.

Il convient dès lors de se poser la question si le Fonds de garantie automobile, qui est censée recevoir de la part de la police grand-ducale copie des procès-verbaux et rapports contenant des données relatives à des infractions pénales, peut légitimement traiter de telles données judiciaires en l'absence de base légale telle qu'exigée par l'article 8 précité. En effet, ce n'est qu'au cas où il existe une véritable base légale ayant pour objet d'autoriser la mise en œuvre de cette catégorie particulière de données dans le chef du Fonds de garantie automobile qu'un règlement grand-ducal pris en exécution de cette loi peut préciser les modalités du traitement autorisé.

Ceci est d'autant plus vrai que le Fonds ne saurait être assimilé à notre avis à une autorité publique, du fait qu'il ne constitue qu'un regroupement de toutes les entreprises d'assurances (cf. art. 15 de la loi du 16 avril 2003).

Il en est autrement pour les informations que le Fonds recueille au titre de l'article 22 de la loi du 16 avril 2003, alors que cette mise à disposition s'effectue sous le contrôle de l'autorité publique qu'est le ministère public et moyennant de garanties appropriées, conformément à l'article 8 paragraphe 2 de la loi du 2 août 2002.

Au vu des dispositions légales et réglementaires difficilement conciliables qui précèdent, la Commission nationale émet des réserves sérieuses quant à la procédure décrite à l'article 18 du règlement grand-ducal du 11 novembre 2003.

Ainsi décidé à Esch-sur-Alzette en date du 17 septembre 2004.

La Commission nationale pour la protection des données

(*s.*) Gérard Lommel	(*s.*) Edouard Delosch	(*s.*) Pierre Weimerskirch
Président	Membre effectif	Membre effectif

Avis de la Commission nationale pour la protection des données concernant le projet de loi n° 5356 relatif aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle

Délibération n°78/2004 du 8 octobre 2004

Conformément à l'article 32, paragraphe 3, lettre (e) de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, la Commission nationale pour la protection des données a entre autres pour mission d'« être demandée en son avis sur 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, et faisant suite à la demande lui adressée par courrier du 26 mai 2004 de Monsieur le Ministre de la Justice, que la Commission nationale entend présenter ci-après plusieurs observations, réflexions et commentaires sur le projet de loi n°5356 relatif aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle.

I. Considérations générales

A) Objectif légitime mais nécessité d'une approche modérée entourée de garanties appropriées

La mise en place de banques de données rassemblant les empreintes génétiques de personnes convaincues de crimes et délits graves a fait l'objet au cours des dernières années d'initiatives législatives dans la plupart de nos pays voisins.

L'empreinte génétique est désormais considérée comme un moyen nécessaire contribuant à élucider les infractions pénales et à en identifier les auteurs.

Limité dans une première phase aux infractions d'ordre sexuel, cet instrument nouveau dans la lutte contre la criminalité a tendance à être étendu à un vaste catalogue d'infractions. L'évolution législative dans les autres pays va dans le sens que le traitement de données génétiques n'est plus limité dorénavant aux malfaiteurs condamnés mais a été étendu progressivement aux personnes soupçonnées, aux victimes, voire à d'autres tiers.

Sans mettre en doute la nécessité pour le législateur luxembourgeois d'instaurer une base juridique pour ce type de données dans le domaine pénal, la Commission nationale tient à faire appel au législateur de faire preuve d'une grande prudence à l'égard de la constitution de fichiers d'empreintes génétiques qui par nature présentent des risques d'atteinte graves aux libertés et droits fondamentaux des personnes physiques, et notamment à leur vie privée.

Conscient du caractère particulièrement sensible des données génétiques, le législateur luxembourgeois a instauré dans la loi du 2 août 2002 un régime très restrictif pour le traitement de cette catégorie particulière de données (cf. article 6 paragraphes 3 et 4 de la loi du 2 août 2002).

En effet, il résulte des travaux parlementaires (projet de loi n° 4735) que « l'article 6 paragraphe 4 de la loi traite des données génétiques pour les soumettre à un régime particulier. Ce régime est plus restrictif que celui des catégories particulières de données, dites données sensibles visées au paragraphe (1) dans la mesure où le traitement de données génétiques n'est possible que dans certains cas bien précis à savoir:

Le traitement est nécessaire à la sauvegarde de la vie de la personne concernée ou d'une autre personne, dans le cas où la personne concernée se trouve dans l'incapacité physique (inclut l'incapacité psychique) ou juridique de donner son consentement; soit

- le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice dès lors qu'il est effectué à cette fin exclusive. Le traitement de données génétiques est encore possible:
- dans le cadre de la réalisation de motifs d'intérêts publics importants, comme ceux de la recherche scientifique, historique, des statistiques publiques;

- dans les hypothèses visées à l'article 17 de la loi (v. nécessité pour la défense, la sûreté de la sécurité publique, activité pénale);
- dans le cadre des articles 6 (3) et 7;
- lorsque le traitement s'appuie sur le consentement de la personne concernée s'il a pour finalité la santé ou la recherche scientifique. Une telle analyse est reprise dans le rapport de Monsieur Guy Braibant (op. cit.). On reprend ici la réserve de l'indisponibilité du corps humain.

L'optique de l'article 6 paragraphe (4) est de limiter a priori au maximum une matière dont les découvertes ne cessent de progresser mais qui à l'heure actuelle ne permet pas encore suffisamment de recul. D'autres textes comme la réglementation européenne sur la brevetabilité du génome viendront probablement interférer. (cf. document parlementaire 4735/00, p. 33 et 34).

Le projet sous avis devrait à son tour refléter la même prudence et veiller à entourer le régime mis en place de mesures de sauvegarde et de garanties appropriées.

B) La structure générale du projet de loi

1) Loi autonome et nouvelles dispositions du code d'instruction criminelle

A l'examen du projet sous avis, l'option retenue par les auteurs du projet consiste, d'une part, à insérer de nouvelles dispositions à différents endroits du Code d'instruction criminelle et, d'autre part, de fixer certaines règles par une loi autonome.

Il ressort du commentaire des articles que « quoiqu'il soit peu usuel que des dispositions du Code d'instruction criminelle soient accompagnées et complétées par une loi autonome, la complexité technique de la matière ADN ainsi que la sensibilité de la question du traitement des données y afférentes justifient cette façon de procéder » (cf. document parlementaire 5356/00, p. 12).

La Commission nationale aimerait d'abord relever que l'agencement du projet sous avis va à l'encontre du choix du législateur de faire régir la matière de la protection des données à caractère personnel par une loi-cadre, à savoir celle du 2 août 2002.

Dans un souci de clarté il aurait été préférable d'insérer les dispositions relatives aux empreintes génétiques, du moins celles faisant partie de ladite « loi autonome », c'est-à-dire celles contenues aux articles 1 à 15 du projet sous avis, dans la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après la loi du 2 août 2002).

Cette approche permettrait une plus grande lisibilité quant à l'articulation des nouvelles dispositions avec celles d'ores et déjà contenues dans la loi du 2 août 2002, en particulier celles relatives aux données judiciaires et aux données génétiques.

L'option retenue par le projet sous avis d'élaborer une loi autonome rendra une lecture harmonieuse des dispositions afférentes moins évidente, voire risque de conduire à des contrariétés de texte ou à des difficultés d'interprétation.

2) Le projet sous avis et son positionnement par rapport à la loi-cadre du 2 août 2002

Le projet sous avis innove en ce qu'il instituera un cadre légal autonome en sus de la loi-cadre du 2 août 2002.

Ne serait-il pas dès lors approprié de préciser dans quelle mesure le projet sous avis entend le cas échéant déroger aux principes établis par la loi du 2 août 2002 ?

Certes il résulte indubitablement du projet sous avis opérant plusieurs renvois à la loi du 2 août 2002 (cf. articles 4 et 8 du projet) ainsi que de l'exposé des motifs (cf. document parlementaire 5356/00, p. 11) que la loi-cadre a vocation à s'appliquer au projet sous avis.

Le projet de loi est toutefois muet sur l'étendue de son champ d'application. En l'absence d'un renvoi général à la loi du 2 août 2002, faut-il en déduire que cette loi s'applique dans toute sa teneur, ou faut-il en dépit de son silence considérer que le nouveau texte y déroge de façon implicite sur certains points.

Aux termes de l'article 3 paragraphe (3) de la loi du 2 août 2002 ladite loi-cadre s'applique aux traitements de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, même liées à un intérêt économique ou financier important de l'Etat, sans préjudice des dispositions spécifiques de droit national ou international régissant ces domaines.

Comme il ressort de l'exposé des motifs ayant conduit à la loi du 2 août 2002 (document parlementaire 4735/00, p. 83), le législateur a en effet opté pour un champ d'application large qui s'étend également aux personnes morales et inclut les domaines de la défense, de la sécurité publique et de la sûreté de l'Etat ainsi que les activités liées au droit pénal en vue d'instaurer un régime juridique unifié capable d'offrir un niveau de sécurité juridique approprié aux personnes concernées.

L'inclusion des quatre matières susvisées (méthode adoptée également par la loi portugaise et en partie par la loi belge) est permise par la Directive 95/46/CE et a été retenu par le législateur luxembourgeois notamment parce qu'elle présente les avantages suivants:

- clarification et unification du régime juridique de la protection des données tout en autorisant à l'Etat de prévoir les limitations et dérogations nécessaires à l'exercice de la puissance publique. Certaines limitations et dérogations sont d'ores et déjà comprises dans le projet de loi. … Les limitations et dérogations prévues par les lois actuellement en vigueur joueront entièrement, dès lors qu'elles touchent aux personnes morales, à la défense, la sécurité publique, la sûreté et aux activités liées au droit pénal. De plus, des lois spéciales pourront à l'avenir édicter de telles limitations et dérogations.
- modifications légères des règlements grand-ducaux existants en la matière …

Les principes du droit relatif à la protection des données s'appliquent donc en règle générale également dans les quatre matières susvisées alors même que la directive 95/46/CE (du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) a exclu de son champ d'application les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal.

Des dérogations aux règles de la loi du 2 août 2002 dans ces domaines, notamment celui des activités de l'Etat liées au droit pénal, sont certes possibles mais devront prendre la forme de dispositions légales et constitueront toujours des exceptions qui seront d'interprétation stricte.

Relevons encore que l'article 13 de la directive 95/46/CE prévoit que les mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 paragraphe 1, à l'article 10, à l'article 11 paragraphe 1 et aux articles 12 et 21 ne peuvent être prises par les Etats membres que lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder:

a) la sûreté de l'État;

b) la défense;

c) la sécurité publique;

d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées.

C) Le prélèvement de cellules humaines exercé sous contrainte physique

Selon le commentaire des articles, en vertu du principe dit de la proportionnalité, il y a lieu de veiller à maintenir l'équilibre entre, d'une part, la gravité de l'intervention sur le corps humain et, d'autre part, les intérêts collectifs et privés en jeu. Il en découle notamment que des prélèvements de cellules humaines ne sauraient être imposés dans le cadre de la poursuite d'infractions mineures.

D'après les auteurs du texte, le principe de proportionnalité a été respecté dans le cadre du présent projet au motif que les dispositions permettant un prélèvement de cellules humaines sous contrainte physique prévoient que ce prélèvement ne peut être effectué que si les faits en cause sont punis d'une peine d'emprisonnement d'un maximum d'au moins deux ans (cf. art. 48-5 paragraphe 3 et 48-8 point 3 ayant trait à l'article 40 deuxième phrase du Code d'instruction criminelle).

Toujours suivant le commentaire des articles, le législateur belge a résolu ce problème en 1999 en retenant la même solution que celle préconisée par le projet sous examen en prévoyant dans le cadre de la loi du 22 mars 1999 la possibilité du prélèvement de cellules humaines sous contrainte physique (cf. document parlementaire 5356/00, p. 13 et 14).

Dans ce contexte, la Commission nationale entend exprimer les observations suivantes :

1) S'il est vrai que le législateur belge a en définitive retenu que l'accord de l'intéressé n'est pas requis pour l'exécution de la mesure, toujours est-il que le recours au système du seuil de la peine (dont s'est inspiré le projet sous avis) est sensiblement différent au Luxembourg.

Contrairement au projet sous avis qui prévoit une peine d'emprisonnement d'un maximum d'au moins deux ans comme seuil minimum permettant le prélèvement contre la volonté de l'intéressé, l'article 3 de la loi belge ne l'impose que dans le cadre de la poursuite d'infractions plus lourdes en partant d'un seuil d'au moins cinq ans d'emprisonnement.

2) Le même constat vaut pour la France où l'article 706-56, paragraphe I, cinquième alinéa, du code de procédure pénale français prévoit un seuil encore plus élevé, « lorsqu'il s'agit d'une personne condamnée pour crime ou pour un délit puni de dix ans d'emprisonnement, le prélèvement peut être effectué sans l'accord de l'intéressé sur réquisitions écrites du procureur de la République. »

Le projet sous avis dépasse donc de loin les seuils de peines retenus par nos pays voisins.

S'agissant des cas où le prélèvement pourra être opéré contre la volonté des personnes concernées, les principes de nécessité et de proportionnalité doivent être appliqués avec d'autant plus de rigueur.

La Commission nationale estime dès lors que le projet sous avis devrait davantage s'inspirer du choix opéré par le législateur belge, voire par le législateur français, qui ont adopté tous les deux une démarche plus modérée pour tempérer le droit fondamental du respect de l'intégrité physique humaine.

D) La surveillance par une autorité de contrôle ?

1) Le procureur général d'Etat : responsable du traitement

Selon le commentaire des articles ayant trait à l'article 6 paragraphe 1er du projet sous avis, « l'autorité la plus appropriée pour être désignée comme responsable du traitement des données en cause est le procureur général d'Etat alors que les données en cause sont des données „judiciaires" au sens de la loi du 2 août 2002 précitée » (cf. document parlementaire 5356/00, p. 19).

Conformément à l'article 2 lettre (o) de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, le « responsable du traitement » est défini comme étant « la personne physique ou morale, l'autorité publique, le service ou tout organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu des dispositions légales, le responsable du traitement est déterminé par ou en vertu des critères spécifiques conformément aux dispositions légales » .

Il résulte des travaux parlementaires (projet de loi n° 4735) que la définition du responsable du traitement désigne « la personne responsable des choix qui président à la définition et à la mise en oeuvre des traitements. Ces choix sont relatifs aux finalités et aux moyens utilisés. Si différentes personnes ou autorités déterminent conjointement ces éléments, elles seront chacune considérées comme responsables » (cf. document parlementaire n° 4735/00, p. 26). Ainsi, « le responsable du traitement dispose du pouvoir décisionnel pour déterminer les finalités poursuivies par un traitement et les moyens à mettre en œuvre en vue de ce traitement. Il se distingue ainsi du sous-traitant chargé de l'exécution matérielle de tout ou partie du traitement » (cf. document parlementaire n° 4735/13, p. 6).

2) Le recours juridictionnel et l'absence d'une autorité de contrôle indépendante

Concernant l'article 15 du projet sous avis, l'on lit dans le commentaire des articles que « cet article vise à conférer une voie de recours aux personnes invoquant la nullité d'un acte posé dans le cadre de la gestion générale des traitements de données ADN criminalistique et condamnés effectuée sous la responsabilité du procureur général d'Etat » et que « l'insertion de cette disposition s'impose principalement par le fait que le responsable de ces traitements de données est le procureur général d'Etat et que la mission de contrôle du responsable de ces traitements ne saurait être exercée par la commission nationale pour la protection des données, instaurée par les articles 32 et suivants de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ». (cf. document parlementaire 5356/00, p. 27).

D'après le commentaire des articles, c'est en raison du fait que les données en cause sont des données „judiciaires" au sens de la loi du 2 août 2002 qu'il paraît justifié de désigner le procureur général d'Etat « comme responsable des traitements de données ADN qui ne permettent guère de soumettre le procureur général d'Etat à la surveillance de cette commission qui est une autorité administrative ne relevant de surcroît pas de la personnalité morale de l'Etat. » (cf. document parlementaire 5356/00, p. 27).

a) La motivation donnée par les auteurs du projet pour faire échapper le procureur général d'Etat à la surveillance de la Commission nationale consistant à dire que cette dernière constitue « une autorité administrative ne relevant de surcroît pas de la personnalité morale de l'Etat » est difficilement compréhensible pour la Commission nationale, puisque sa création comme autorité de contrôle indépendante, tant vis-à-vis des acteurs du secteur privé que du secteur public, était une des exigences-clés de la directive 95/46/CE pour assurer une meilleure protection des droits des personnes concernées.

En effet, aux termes de l'article 28 paragraphe 1er de la directive 95/56/CE « Chaque Etat membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les Etats membres en application de la présente directive. Ces autorités exercent en toute indépendance les missions dont elles sont investies. »

Aux yeux de la Commission nationale, une telle motivation ne constitue guère un argument pertinent pour ne pas soumettre le traitement opéré sous la responsabilité du procureur général d'Etat - mais qui en pratique sera pour l'essentiel effectué par la police grand-ducale pour son compte – à la surveillance d'une autorité de contrôle en matière de protection de la vie privée et des données personnelles.

Elle estime que le seul motif qui puisse tout au plus valablement justifier ce choix est celui de la séparation des pouvoirs qui interdit qu'une autorité administrative puisse contrôler le troisième pouvoir (à savoir le pouvoir judiciaire) qui est indépendant.

Concernant le traitement de donnes judiciaires (article 8 de la loi du 2 août 2002), il est intéressant de citer dans ce contexte un extrait de l'avis du Procureur général d'Etat émis à l'occasion du projet de loi n°4735 qui s'est également posé la question au sujet des responsabilités respectives des autorités judiciaires et de la Commission nationale :

« Il faudrait également préciser les responsabilités respectives des autorités judiciaires qui créent et gèrent les traitements en cause et de la Commission nationale. Pour les traitements de données relatives à des affaires en cours, notamment en matière pénale, on peut sérieusement s'interroger sur un contrôle exercé par la Commission nationale et sur un accès indirect au profit des personnes visées. » (cf. document parlementaire n° 4735/02, p. 2, document retiré par la suite à la demande de Monsieur le Ministre délégué aux Communications).

b) L'article 8 paragraphe 5 de la directive prévoit que « Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'Etat membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.»

Le législateur luxembourgeois a créé lors de la transposition de la directive deux autorités de contrôle en matière de protection des données, l'une ayant une compétence générale que l'on pourrait qualifier de droit commun, c'est-à-dire la Commission nationale instituée en vertu de l'article 34 de la loi du 2 août 2002, l'autre ayant une mission spécifique à remplir consistant à surveiller les « données de police » visées à l'article 17 de la loi, en l'occurrence l'autorité de contrôle instaurée sur base de l'article 17 de la loi du 2 août 2002.

Si la mission de surveillance de l'autorité de contrôle prévue à l'article 17 de la loi est strictement cantonnée aux traitements édictés à l'article 17, la Commission nationale a vocation générale pour toutes les autres matières régies par la loi-cadre.

Le projet sous avis prévoit seul un recours juridictionnel individuel de la part de la personne concernée (f. article 15 du projet).

Or, il paraît inconcevable qu'un régime légal puisse être institué pour des données génétiques par nature hautement sensibles dont le traitement est particulièrement invasif pour la vie privée de la personne concernée, sans que le traitement envisagé soit soumis à une surveillance efficace de la part d'une autorité de contrôle indépendante qui puisse agir de sa propre initiative, indépendamment des droits individuels conférés par ailleurs à la personne concernée.

c) Dans ce contexte, il est encore intéressant de relever que l'article R53-17 du code de procédure pénale français fait expressément état, à côté des pouvoirs réservés au magistrat compétent, des pouvoirs conférés à la CNIL, soit l'autorité de contrôle en matière de protection des données :

« Le magistrat mentionné à l'article R. 53-16 et, à sa demande, les membres du comité prévu au même article disposent d'un accès permanent au fichier et au lieu où se trouve celui-ci.

L'autorité gestionnaire du fichier lui adresse un rapport annuel d'activité ainsi que, sur sa demande, toutes informations relatives au fichier.

Ce magistrat peut ordonner toutes mesures nécessaires à l'exercice de son contrôle, telles que saisies ou copies d'informations, ainsi que l'effacement d'enregistrements illicites.

Les pouvoirs qui lui sont confiés s'exercent sans préjudice du contrôle exercé par la Commission nationale de l'informatique et des libertés en application des dispositions et selon les modalités prévues par l'article 21 de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. »

E) Droits de la personne concernée

Dans ce contexte, se pose également la question relative aux droits de la personne concernée (droit à l'information, droit d'accès et droit d'opposition), inscrits aux articles 26 et suivants de la loi du 2 août 2002.

1) Le droit à l'information

Le droit à l'information de la personne concernée est consacré dans une hypothèse bien déterminée, prévue à l'article 16 du projet sous avis relatif au nouvel article 48-5 du code d'instruction criminelle.

Il serait judicieux de préciser que ce droit à l'information, qui constitue un élément fondamental de la protection de personnes à l'égard du traitement des données à caractère personnel, répond aux exigences posées à l'article 26 de la loi du 2 août 2002 et comprend les informations y mentionnées.

Par ailleurs, les informations figurant dans l'accord écrit de la personne concernée au titre de l'article 48-5 paragraphe 2 du projet sous avis ne doivent pas se borner à faire un simple renvoi aux dispositions légales en cause, notamment aux articles 48-6 paragraphes 1 à 3, mais la personne concernée doit obtenir une information sous forme lisible et intelligible conformément au vœu de la directive 95/46/CE.

Pour le surplus, les auteurs du projet sous avis semblent considérer que le droit à l'information n'est pas applicable, sans pour autant le dire expressément en renvoyant à une des exceptions prévues à l'article 27 de la loi du 2 août 2002, telle que la lettre d), alors que le paragraphe 3 de l'article 48-5 ne fait pas état du droit à l'information dans le chef des personnes sur lesquelles un prélèvement peut être effectué sous contrainte physique.

La Commission nationale s'interroge sur la nécessité de priver les personnes paraissant présenter un lien direct avec la réalisation des faits du droit à l'information, sauf dans les cas où une telle information risquerait de compromettre le succès de l'instruction pénale.

2) Le droit d'accès

Le projet sous avis garde le silence sur la manière et auprès de quelle autorité le droit d'accès peut être exercé par la personne concernée

Si la loi du 2 août 2002 prévoit la possibilité d'écarter le droit à l'information dans certains cas, il en va autrement pour le droit d'accès.

En effet, l'article 29 de la loi du 2 août 2002 énonce que le responsable du traitement ne peut que limiter ou différer l'exercice du droit d'accès d'une personne concernée lorsqu'une telle mesure est nécessaire pour sauvegarder certains intérêts limitativement énumérés.

Il en suit qu'une exclusion totale du droit d'accès serait contraire à la loi du 2 août 2002.

La Commission nationale estime qu'en raison de la sensibilité des données collectées, ce droit fondamental appartenant à la personne concernée devrait être consacré dans le projet sous avis.

A noter que l'article R53-15 du code de procédure pénale français fait expressément référence au droit d'accès réservé à la personne concernée en prévoyant que, « le droit d'accès prévu par l'article 34 de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés s'exerce auprès du directeur central de la police judiciaire au ministère de l'intérieur ».

3) Le droit d'effacement

A noter que l'article 706-54 du code de procédure pénale français (partie législative) octroie en plus un droit d'effacement à certaines catégories de personnes concernées :

« Les empreintes génétiques des personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions mentionnées à l'article 706-55 sont également conservées dans ce fichier sur décision d'un officier de police judiciaire agissant soit d'office, soit à la demande du procureur de la République ou du juge d'instruction ; il est fait mention de cette décision au dossier de la procédure. Ces empreintes sont effacées sur instruction du procureur de la République agissant soit d'office, soit à la demande de l'intéressé, lorsque leur conservation n'apparaît plus nécessaire compte tenu de la finalité du fichier. Lorsqu'il est saisi par l'intéressé, le procureur de la République informe celui-ci de la suite qui a été réservée à sa demande ; s'il n'a pas ordonné l'effacement, cette personne peut saisir à cette fin le juge des libertés et de la détention, dont la décision peut être contestée devant le président de la chambre de l'instruction. »

Par ailleurs, l'article R53-13-1 du code de procédure pénale français accorde un droit d'effacement à d'autres catégories de personnes concernées :

« Le procureur de la République compétent pour, en application des dispositions du deuxième alinéa de l'article 706-54, ordonner d'office ou à la demande de l'intéressé l'effacement de l'enregistrement d'un résultat mentionné au 2º du I de l'article R. 53-10 est celui de la juridiction dans le ressort de laquelle a été menée la procédure ayant donné lieu à cet enregistrement.

La demande d'effacement prévue par le deuxième alinéa de l'article 706-54 doit, à peine d'irrecevabilité, être adressée par lettre recommandée avec demande d'avis de réception ou par déclaration au greffe. Cette demande est directement adressée au procureur de la République mentionné à l'alinéa précédent. Elle peut également être adressée au procureur de la République du domicile de l'intéressé, qui la transmet au procureur de la République compétent.

Le procureur de la République compétent fait droit à la demande d'effacement lorsqu'elle est présentée par une personne mentionnée au 5º de l'article R. 53-10. »

Suivant le point 5º de l'article R. 53-10 du code de procédure pénale français, il s'agit « 5º des échantillons biologiques prélevés, avec leur accord, sur les ascendants et descendants d'une personne disparue, dans le cadre d'une enquête ou d'une instruction pour recherche des causes d'une disparition inquiétante ou suspecte prévue par les articles 74-1 ou 80-4. »

La Commission nationale estime que pareil droit d'effacement devrait également être introduit dans le projet de loi sous avis, puisqu'un aspect de la proportionnalité réside précisément dans une durée de conservation proportionnée à la finalité poursuivie (cf. article 4 paragraphe 1er lettre d) de la loi du 2 août 2002).

Dans ce même ordre d'idée, il y a lieu de se rapporter à nos commentaires afférents au sujet de l'article 10 du projet sous avis.

4) Le droit de rectification

Aux termes de l'article 4 paragraphe 1er lettre c) de la loi du 2 août 2002, le responsable du traitement doit s'assurer que les données qu'il traite sont exactes et, si nécessaire, mises à jour; toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

La Commission nationale préconise de compléter le projet sous avis par l'introduction d'un tel droit de rectification dont l'attribution à la personne concernée s'impose comme dans les situations de droit commun et même davantage dans la mesure où la catégorie particulière de données collectée peut engendrer des répercussions négatives, voire infamantes pour la vie privée des personnes fichées.

A noter qu'en vertu de l'article 29 paragraphe 4 de la loi du 2 août 2002, « en cas de limitation de l'exercice du droit d'accès de la personne concernée, le droit d'accès est exercé par la Commission nationale qui dispose d'un pouvoir d'investigation en la matière et qui fait opérer la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente loi. La Commission nationale peut communiquer à la personne concernée le résultat de ses investigations, sans toutefois mettre en danger la ou les finalités des traitements en question. »

F) Sécurité des traitements

1) « S'agissant des mesures de sécurité particulièrement impérieuses qui doivent entourer un fichier de cette nature, seuls des fonctionnaires de la sous-direction de la police technique et scientifique du ministère de l'Intérieur et les personnels de l'Institut de recherche criminelle de la Gendarmerie nationale, spécialement habilités et affectés au service mettant en œuvre le traitement, pourront procéder aux opérations de rapprochement entre une empreinte génétique résultant de l'analyse effectuée dans le cadre d'une recherche criminelle pour l'une des infractions sexuelles visées par l'article 706-47 du code pénal et les empreintes enregistrées dans le fichier, une traçabilité des consultation par suivi informatique étant bien évidemment mise en place. Enfin, dans le souci d'éviter toute erreur dans la saisie de la série de chiffres qui constitue l'empreinte génétique, une double saisie sera effectuée par deux opérateurs distincts avant tout enregistrement au fichier national. » (cf, 20e rapport d'activité pour l'année 1999 de la CNIL, le fichier national des empreintes génétiques, p. 35).

« L'article 5 vise également à assurer la protection et la confidentialité des traitements de données ADN. En effet, il ne saurait être admis que ces données puissent être consultées sans motif ou pour des motifs non liés à la poursuite d'une infraction. Dans cet ordre d'idées, les informations visées par cet article doivent être enregistrées lors de chaque consultation ou comparaison, afin de pouvoir retracer quand, par qui et pour quels motifs un profil d'ADN a fait l'objet d'un traitement. » (cf. document parlementaire 5356/00, p. 18).

S'il est vrai que les mesures envisagées à l'article 5 du projet sous contribueront à assurer une meilleure sécurité des traitements, il n'en demeure pas moins qu'aux yeux de la Commission nationale elles s'avèrent insuffisantes pour satisfaire aux conditions édictées au chapitre V de la loi du 2 août 2002 relatif à la confidentialité et à la sécurité des traitements.

Le projet sous avis devrait comporter des dispositions spécifiques au sujet des mesures de sécurité particulières à prendre par le responsable du traitement, en l'occurrence le procureur général d'Etat.

Conformément à l'article 22 paragraphe 1er de la loi du 2 août 2002, le responsable du traitement doit mettre en œuvre toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

2) La Commission nationale aimerait encore attirer l'attention aux sources potentielles d'erreurs et à l'assurance qualité à assurer dans le domaine de l'expertise d'ADN en droit criminel en se référant à un extrait d'un article intitulé « L'EXPERTISE D'ADN EN DROIT CRIMINEL : CE QU'IL FAUT SAVOIR » de Danielle Desmarais, Ph.D., Dr Lambert Busque, MD., FRCPC (professeur agrégé de médecine, Université de Montréal et président de PROADN Diagnostic inc., en collaboration avec Danielle Desmarais, Ph.D., directrice scientifique, PRO-ADN Diagnostic inc.) :

« Lorsque l'analyse d'ADN est réalisée dans des conditions optimales, elle permet une identification des plus fiable et des plus précise. Cependant, comme dans toutes techniques sophistiquées exigeant de longues et complexes manipulations, l'erreur humaine ou technique est possible. Il importe donc de s'assurer que les normes préventives, les protocoles rigoureux et les contrôles de qualité sont respectés par tous les intervenants, que ce soit au niveau de la cueillette des échantillons, de la préparation de l'ADN, de l'analyse proprement dite et de l'interprétation des résultats.

Tableau II — Sources potentielles d'erreurs

Source	Lieu	Intervenant
Collecte de spécimens	Scène du crime	Policier, enquêteur
Préparation des spécimens	Laboratoire	Technicien
Procédure d'analyse équipement	Laboratoire	Technicien, expert,
Interprétation des résultats	Laboratoire	Expert
Calcul des probabilités	Laboratoire	Expert

1. Échantillonnage

Une chaîne de possession claire et bien documentée doit être maintenue dès la cueillette des échantillons. Les échantillons doivent être manipulés, analysés et conservés de manière à les protéger contre la perte, les changements néfastes et les risques de contamination. À cause de sa très grande sensibilité, la technique PCR est sensible à la contamination par des sources d'ADN extérieures, comme l'ADN du manipulateur (policier et technicien de laboratoire) ou l'échange de matériel génétique d'un prélèvement à un autre. Ainsi, chaque évidence biologique ou échantillon d'ADN devrait être subdivisé afin d'en conserver une portion non-manipulée, pour des fins de contre-expertise si cela s'avère nécessaire.

2. Procédure analytique

Toutes les étapes de la procédure d'analyse doivent être contrôlées et documentées de façon rigoureuse. De multiples systèmes de contrôle de qualité doivent être mis en place afin de détecter les problèmes techniques (équipements, réactifs), de contamination (contrôles expérimentaux) et ceux relatifs à la qualité de l'ADN. Toutes ces mesures permettent d'assurer l'exactitude des résultats. De plus, l'expert doit être en mesure de faire les choix qui s'imposent autant au niveau des techniques à utiliser (RFLP vs PCR) que des méthodes de travail afin de ne pas détruire la preuve et de maximiser les chances de réussite.

3. Interprétation des résultats

L'interprétation des résultats est une étape importante qui demande beaucoup de rigueur scientifique et une expérience certaine. Elle doit se faire en tenant compte des limites technologiques et scientifiques ainsi que des contrôles de qualité. De façon inconsciente ou consciente, l'interprétation des résultats peut être biaisée, soit à cause des artefacts (quantité ou qualité de l'ADN sous-optimale), soit à cause d'une fausse association en raison de la présence de contributeurs multiples dans l'échantillon, soit à cause de la sélection de résultats en voulant écarter un résultat discordant ou disculpant ou en mettant de côté certaines évidences biologiques. Il faut donc être prudent face au manque d'objectivité car des conclusions prématurées pourraient avoir des conséquences graves.

4. Calcul des probabilités

Les calculs des probabilités sont basés sur des concepts génétiques complexes qui doivent être bien maîtrisés par l'expert. À cet effet, les calculs varient selon que le profil génétique, à un locus particulier, est hétérozygote (Aa), homozygote (AA, aa) ou mixte (plusieurs contributeurs). Afin, de ne pas évaluer de façon erronée la probabilité d'une concordance positive entre deux profils génétiques, une grande précaution demeure de rigueur, principalement lorsqu'il s'agit d'échantillons à contributeurs multiples. De plus, l'analyse statistique n'aura une signification que si on utilise des bases de données pertinentes. »

II. Les dispositions essentielles du projet de loi sous avis

Les dispositions essentielles du projet de loi sous avis qui soulèvent des questions relatives à la protection des personnes à l'égard du traitement de données à caractère personnel sont les suivantes :

A) Article 3 : l'expert chargé de l'établissement du profil d'ADN

Il résulte du commentaire des articles que « Plusieurs raisons font en effet qu'il y a lieu de s'inspirer de ces textes : tout d'abord, les méthodes d'analyses utilisées dans divers pays européens se font selon les mêmes procédures techniques et beaucoup d'analyses de cellules humaines prélevées au Luxembourg, surtout à l'heure actuelle et certainement encore dans une première phase après l'entrée en vigueur de la présente loi, seront exécutées dans les laboratoires des pays voisins, de sorte que la reprise des principes élémentaires en usage dans ces pays facilitera cette pratique. (cf. document parlementaire 5356/00, p. 16).

Si l'article 3 introduit certaines règles élémentaires concernant la procédure d'analyse dans le but d'assurer la plus grande qualité possible des profils d'ADN établis, toujours est-il que cet article passe sous silence les qualités auxquelles doit répondre l'expert y chargé de procéder à l'établissement du profil d'ADN.

Contrairement au projet sous avis, l'article 2 de la loi belge du 22 mars 1999 prévoit la désignation d'un expert « attaché à un laboratoire agréé par le Roi » et l'article 7 dispose encore qu'un règlement détermine les « modalités relatives à l'agréation des laboratoires et à la possibilité de requérir des laboratoires étrangers » et fixe les garanties particulières en matière de confidentialité et de protection des données à caractère personnel.

Il conviendrait dès lors de préciser si l'expert visé est un expert assermenté choisi sur la liste officielle des experts judiciaires, voire d'entourer sa désignation de garanties appropriées en raison des données traitées en cause, par nature très sensibles.

B) Article 4 : un profil ADN constitue-t-il une donnée à caractère personnel ?

1) La notion de donnée à caractère personnel

a) Une donnée personnelle est une information permettant d'identifier ou rendant identifiable la personne concernée par cette donnée.

D'après le considérant 26 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données :

«Les principes de la protection doivent s'appliquer à toute information concernant une personne identifiée ou identifiable; que, pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en oeuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne... ».

Le Comité des Ministres du Conseil de l'Europe a récemment rappelé lors d'une Recommandation adoptée le 18 septembre 2002, lors de la 808e réunion des Délégués des Ministres Rec (2002)9 et relative à la protection des données à caractère personnel collectées et traitées à des fins d'assurance (CONSEIL DE L'EUROPE COMITE DES MINISTRES, Recommandation Rec (2002)9 du Comité des Ministres aux Etats membres sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance (http://cm.coe.int/stst/F/Public/2002/adopted_texts/recommendations/f2002r9.htm) que:

"a. L'expression « données à caractère personnel » englobe toute information concernant une personne physique identifiée ou identifiable (« personne concernée »). Une personne physique n'est pas considérée comme « identifiable » si cette identification nécessite des délais et des activités déraisonnables. "

Il en suit qu'une personne est identifiable si des moyens raisonnables suffisent. Ces moyens peuvent être utilisés tant par la personne qui traite ces informations que par un tiers. La qualification de moyen raisonnable doit être mise en perspective avec les moyens technologiques de plus en plus poussés à disposition des personnes qui traitent des informations. Il appartient naturellement aux autorités de contrôle de définir la limite du moyen raisonnable.

L'article 2 a) de la Directive 95/46/CE, tout en reprenant l'essentiel du considérant 26 ajoute une présomption:

"Aux fins de la présente directive, on entend par:

a) «données à caractère personnel»: toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale; "

De plus, est présumée identifiable, la personne se rattachant à un numéro d'identification ou à une ou plusieurs informations propres à son identité.

Cette présomption est reprise dans la loi du 2 août 2002 et amplifiée puisqu'on y fait aussi référence aux informations génétiques. Cet ajout se justifie, tout d'abord parce que le patrimoine génétique est un élément propre de chaque individu, ensuite, parce que la loi intègre la question des données génétiques ce que ne fait pas spécifiquement la directive 95/46/CE (sans pour autant les exclure).

Aux termes de la lettre (e) de l'article 2 de la loi, la "donnée à caractère personnel" est définie comme étant « toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable ("personne concernée"); une personne physique ou morale est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ».

Enfin, la loi luxembourgeoise, ajoute une présomption de caractère propre pour les données génétiques.

En résumé, une donnée est à caractère personnel si quelqu'un peut, par l'utilisation de moyens raisonnables et appropriés identifier la personne qui se cache derrière cette donnée. Elle sera réputée à caractère personnel si elle fait référence à son numéro d'identification ou à un caractère propre de la personne (physique, physiologique, génétique, psychique, économique, culturelle ou sociale).

A noter que la donnée génétique a été définie à l'article 2, lettre g), de la loi du 2 août 2002 comme étant « toute donnée concernant les caractères héréditaires d'un individu ou d'un groupe d'individus apparentés », et que la lettre f) de l'article 2 ajoute que la "donnée relative à la santé" vise toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques.

La définition de la „ donnée génétique" (art. 6 (1) (b)) en question est reprise de la Recommandation No R (97) 5 du 13 février 1997 du comité des ministres du Conseil de l'Europe relative à la protection des données médicales. La définition précise, que la donnée génétique „se réfère également à toute donnée portant sur l'échange de toute information génétique (gènes) concernant un individu ou une lignée génétique, en rapport avec les aspects, quels qu'ils soient, de la santé ou d'une maladie, qu'elle constitue ou non un caractère identifiable", la lignée génétique étant considérée comme la lignée „constituée par des similitudes génétiques résultant d'une procréation et partagées par deux ou plusieurs individus". " (cf. document parlementaire 4735/00, p. 32).

Cependant, d'après les travaux parlementaires, toute donnée génétique quel que soit son caractère scientifique n'est pas nécessairement relative à la santé. Par exemple le gène récessif ou dominant déterminant la couleur des cheveux ou celui déterminant leur nombre ne pourra pas a priori être classé dans la catégorie des données relatives à la santé de la personne concernée. Ceci justifie la distinction entre ces deux notions tant au niveau des définitions que dans la structure des articles 6 et 7 de la loi. (cf. document parlementaire 4735/00, p. 94).

b) Il ressort encore des travaux parlementaires (projet de loi n° 4735) que les auteurs Marie-Hélène Boulanger, Cécile de Terwangne, Thierry Léonard, Sophie Louveaux, Damien Moreau et Yves Poullet, dans leur dossier „La protection des données à caractère personnel en droit communautaire", paru dans le Journal des Tribunaux – Droit européen, juin 1997, considèrent que „dès lors que, techniquement, in abstracto, un moyen existe de rendre les personnes concernées identifiables, elles sont réputées telles par la définition. Le caractère identifiable apparaît alors comme relatif eu égard aux possibilités d'identification du ou des responsables" [du traitement]. „Il revient (…) à la personne qui traite les données et qui considère ne pas devoir respecter les principes protecteurs, de rapporter la preuve du caractère anonyme de celles-ci dans son chef; en présentant toute garantie utile quant à la conservation du caractère anonyme des données (…)." (cf. document parlementaire 4735/00, p. 25).

c) Reproduisons dans ce contexte en outre un extrait du document de travail sur les données génétiques du groupe de protection des personnes à l'égard du traitement des données à caractère personnel (« groupe 29 ») dans le cadre du WP 91 1/97, adopté par le groupe le 17 mars 2004 (voir sous le hyperlien http://europa.eu.int/

comm/internal_market/privacy/docs/wpdocs/2004/wp91_fr.pdf

« Il ne fait aucun doute que les informations génétiques sont couvertes par cette définition. En effet, le lien avec une personne donnée, c'est-à-dire le fait que la personne concernée est identifiée ou identifiable, est évident dans la majorité des cas. Il reste que, dans certains cas, ce n'est pas aussi clair, comme en ce qui concerne les échantillons d'ADN prélevés sur le lieu d'un crime. Toutefois, ce type d'échantillons est susceptible de constituer une source de données personnelles puisqu'il peut être possible d'associer des échantillons d'ADN à une personne donnée, surtout lorsque leur origine a été confirmée par un tribunal sur la base des preuves scientifiques. C'est pourquoi la réglementation en matière de données génétiques doit également examiner le statut juridique des échantillons d'ADN (cf. p. 5 du document) ».

2) Le profil ADN

D'après l'article 4 (2) du projet sous avis « Un profil d'ADN établi est à considérer comme donnée à caractère personnel, au sens de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, à partir du moment où le code alphanumérique de l'analyse d'ADN a été associé à une information relative à la personne physique en cause permettant de l'identifier. ».

La Commission nationale ne saurait partager ce point de vue. Elle se rallie sur ce point à l'avis de la Commission belge pour la protection de la vie privée rendu sur l'avant-projet de loi relatif à l'analyse ADN en matière pénale en Belgique :

« 11. Les profils ADN constituent des données à caractère personnel, même s'ils ne sont pas encore identifiés. En effet, les données à caractère personnel sont des données relatives à une personne physique identifiée ou identifiable. Chaque profil ADN peut en principe être identifié. L'identification des personnes constitue d'ailleurs la finalité explicite de ces traitements de données.

12. Dans la mesure où, dans l'état actuel de la science, aucune donnée concernant la santé ne peut être déduite à partir de segments d'ADN non codants, ces données ne constituent pas des données médicales au sens de l'article 7 de la loi du 8 décembre 1992 (loi relative aux traitements de données à caractère personnel, ci-après LTDP). Aussi, la surveillance d'un praticien de l'art de guérir n'est-elle pas requise. Il convient toutefois de souligner que l'article 1er, alinéa 2 de la recommandation R (97) 5 inclut de manière générale les données génétiques dans les données médicales. Il n'est, en effet, pas exclu qu'à terme, l'on puisse également déduire des données médicales à partir des segments d'ADN non codants.

En fonction des données complémentaires qui sont enregistrées dans les banques de données, il convient de considérer qu'il s'agit également de traitements de données judiciaires. Les données enregistrées dans la banque de données "Condamnés", qui contient les profils ADN de personnes condamnées du chef de certaines infractions, doivent certainement être considérées comme des données judiciaires. » (cf. avant-projet de loi relatif à l'analyse ADN en matière pénale ; Commission pour la protection de la vie privée, Belgique, Numéro : JZ985ED_1, Numéro de rôle : 17/98 du 14 mai 1998.)

C) Article 6 paragraphe 2 : les interconnexions prévues par la loi

Aux termes du second paragraphe de l'article 6 du projet sous avis, « les traitements ADN criminalistique et ADN condamnés ne peuvent faire l'objet d'aucune interconnexion, entre eux ou avec d'autres traitements de données à caractère personnel, autre que celles prévues par la présente loi. »

La Commission nationale salue l'approche du gouvernement d'utiliser le terme „interconnexion" dans le même sens suivant lequel il est utilisé aux articles 2 litt. (j) et 16 de la loi-cadre du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (cf. document parlementaire n° 5356/00, p. 20).

Elle se demande toutefois, au vu du projet sous avis, quelles sont les interconnexions expressément instaurées par le projet sous avis, alors que le terme « interconnexion » ne figure qu'à l'article 6.

S'agit-il des « comparaisons » évoquées dans plusieurs articles (articles 5, 10, 12 et 16) ? A noter que le terme « comparaison » n'est d'ailleurs pas expressément mentionné comme une opération spécifique de traitement de données au sens de la notion de « rapprochement » telle que visée à l'article 2 lettre s) de la loi du 2 août 2002.

Au niveau du commentaire des articles, il est écrit dans ce contexte que « dans le cadre du présent projet, le terme de „consultation" vise plutôt la vérification ou le rapprochement d'un profil d'ADN déterminé à un autre, notamment par voie manuelle, tandis que le terme „comparaison" vise plutôt une comparaison systématique d'un grand nombre de profils d'ADN par le biais d'un outil informatique. » (cf. document parlementaire n° 5356/00, p. 18).

Le projet sous avis devrait donc énumérer de façon précise quelles interconnexions il entend autoriser par voie légale, étant donné que l'article 16 de la loi du 2 août 2002 dispose en son paragraphe 1er que « l'interconnexion de données qui n'est pas expressément prévue par un texte légal doit faire l'objet d'une autorisation préalable de la Commission nationale sur demande conjointe présentée par les responsables des traitements en cause ».

Au cas où une demande d'autorisation préalable ayant pour objet une interconnexion de données est introduite auprès de la Commission nationale, celle-ci doit examiner la licéité du traitement et les garanties concernant la compatibilité des finalités des traitements à interconnecter au regard du cadre légal prescrit à l'article 16 de la loi du 2 août 2002 (cf. document parlementaire n° 4735/8, p. 10 ; amendements adoptés par la commission des medias et des communications).

En revanche, si le législateur entend - comme en l'espèce - autoriser une interconnexion de données par une loi, il résulte des travaux parlementaires relatifs au projet de loi ayant mené à la loi du 2 août 2002 que « l'élaboration de textes législatifs ou réglementaires autorisant une interconnexion de données devraient s'inspirer de la ratio des dispositions de l'article 16 » (document parlementaire 4735/13, p. 30 ; rapport de la commission des medias et des communications).

D) Articles 48-3 et 48-5 nouveaux du code d'instruction criminelle

Selon le commentaire des articles au sujet de l'article 48-3 nouveau du code d'instruction criminelle « La formule „… personnes concernées par une infraction…" a été choisie à dessein afin de permettre d'établir un profil d'ADN dans un large éventail de cas de figure. L'idée est de rendre possible, par exemple, d'établir les profils d'ADN de personnes qui se sont trouvées dans des conditions spatio-temporelles particulières par rapport à la commission de l'infraction (un groupe de personnes qui étaient toutes présentes peu avant la commission des faits dans l'appartement où un cadavre a été découvert, les habitants d'un village aux bords duquel une fille a été retrouvée morte et violée, les profils d'ADN de certains membres de la famille d'une victime disparue sont nécessaires pour établir si des cellules humaines retrouvées appartiennent à la victime en cause, etc.).(cf. document parlementaire n° 5356/00, p. 29).

Selon le commentaire des articles, la formulation retenue à l'article 48-5 paragraphe (3) nouveau du projet „… personne paraît présenter un lien direct avec la réalisation des faits en cause …" « est inspirée de l'article 90undecies § 1er du Code d'instruction criminelle belge tel que celui-ci y a été introduit par l'article 5 de la loi du 22 mars 1999 et signifie en fait que le prélèvement sous contrainte peut être effectué également sur des personnes qui ne sont pas, ou pas encore, considérées comme suspects mais qui sont néanmoins impliquées dans la genèse des faits, comme la victime, ou une personne ayant été sur les lieux du crime peu avant sa commission. Or, si ce principe peut faire croire à première vue à une application trop large de la technique d'ADN, elle permet cependant aussi de disculper des innocents et, surtout, d'orienter une enquête dès le début dans la bonne direction. »

Il appert que la formulation employée à l'article 48-3 paragraphe (1) „… personnes concernées par une infraction…" est distincte de celle „… personne paraît présenter un lien direct avec la réalisation des faits en cause …" utilisée à l'article 48-5 paragraphe (3) du projet.

Quant à la première catégorie, le traitement ne sera possible qu'avec le consentement de la personne concernée, tandis que pour la seconde catégorie un prélèvement sous contrainte physique peut être effectué sur la personne concernée.

L'intention du législateur vise donc à limiter davantage les hypothèses dans lesquelles un prélèvement sous contrainte physique peut être opéré au motif qu'une « personne concernée par une infraction » n'est pas ipso facto aussi une personne qui « paraît présenter un lien direct avec la réalisation des faits en cause ».

La Commission nationale ne peut que saluer l'approche restrictive adoptée par le projet sous avis. Comme l'a relevé à juste titre la Commission belge pour la protection de la vie privée dans son avis rendu sur l'avant-projet de loi relatif à l'analyse ADN en matière pénale en Belgique, un recensement collectif de profils ADN ne devrait être possible que sur base d'une participation volontaire de la population concernée. La Commission belge critiquait qu'une telle collecte puisse être imposée sous contrainte physique en citant justement le même exemple que celui évoqué dans le projet sous avis :

« …dans le cadre d'une affaire locale de viol, soumettre l'ensemble de la population masculine d'un village à une analyse ADN est considéré comme étant une application disproportionnée. » (cf. avant-projet de loi relatif à l'analyse ADN en matière pénale ; Commission pour la protection de la vie privée, Belgique, Numéro : JZ985ED_1, Numéro de rôle : 17/98 du 14 mai 1998.)

Tel que les deux articles susmentionnés sont rédigés, il semble que l'intention du législateur soit celle de recueillir le consentement de la population concernée en cas d'un recensement collectif de profils ADN, de sorte que sous ce rapport le principe de proportionnalité est respecté.

Pour enlever tout malentendu, il serait peut-être opportun de préciser expressément dans le projet de loi que cette formulation est à distinguer de celle retenue au niveau de l'article 48-3 „… personnes concernées par une infraction…".

La Commission nationale se montre toutefois préoccupée devant le risque de voir un grand nombre de personnes innocentes forcées à se soumettre à un prélèvement de leur profil ADN au titre de l'article 48-5 nouveau du code d'instruction criminelle, étant donné que la notion de „… personne paraît présenter un lien direct avec la réalisation des faits en cause …" reste un critère de délimitation assez vague qui s'avérera difficile à manier par les autorités publiques lors de sa mise en oeuvre concrète.

Contrairement au projet sous avis, l'article 706-54 du code de procédure pénale français (partie législative) adopte une autre approche, plus mesurée, en énumérant limitativement les personnes dont les empreintes génétiques peuvent être centralisées dans le fichier national.

D'après le texte français, il s'agit grosso modo des cas d'ouverture suivants :

« Le fichier national automatisé des empreintes génétiques, placé sous le contrôle d'un magistrat, est destiné à centraliser les empreintes génétiques issues des traces biologiques ainsi que les empreintes génétiques des personnes condamnées pour l'une des infractions mentionnées à l'article 706-55 en vue de faciliter l'identification et la recherche des auteurs de ces infractions.

Les empreintes génétiques des personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions mentionnées à l'article 706-55 sont également conservées dans ce fichier sur décision d'un officier de police judiciaire agissant soit d'office, soit à la demande du procureur de la République ou du juge d'instruction ; il est fait mention de cette décision au dossier de la procédure….

Les officiers de police judiciaire peuvent également, d'office ou à la demande du procureur de la République ou du juge d'instruction, faire procéder à un rapprochement de l'empreinte de toute personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis un crime ou un délit, avec les données incluses au fichier, sans toutefois que cette empreinte puisse y être conservée.

Le fichier prévu par le présent article contient également les empreintes génétiques issues des traces biologiques recueillies à l'occasion des procédures de recherche des causes de la mort ou de recherche des causes d'une disparition prévues par les articles 74, 74-1 et 80-4 ainsi que les empreintes génétiques correspondant ou susceptibles de correspondre aux personnes décédées ou recherchées…. »

Force est de constater que l'empreinte génétique de simples témoins ou d'autres personnes innocentes ne sera pas enregistrée en France.

E) Article 9 paragraphe 3 : comparaison négative

« En revanche, et l'alinéa 2 du paragraphe (3) (de l'article 9) le précise, si ces comparaisons ont été négatives, cela revient à dire que l'intéressé n'est ni impliqué dans l'affaire en cause, ni dans une autre enquête préliminaire ou instruction préparatoire d'ailleurs, et n'a encore jamais été condamné pour une des infractions prévues à l'article 48-7 du Code d'instruction criminelle. Dans ce cas, il n'y a aucune raison qui pourrait justifier que le profil d'ADN de cette personne figure au traitement ADN criminalistique; la conséquence en est que ce profil d'ADN ne peut plus faire l'objet d'un traitement ADN dans la suite, ni „criminalistique", ni „condamnés"» (cf. document parlementaire n° 5356/00, p. 21).

La Commission nationale regrette que cet article n'indique pas à l'abri de tout doute si les profils ADN obtenus sur base volontaire à l'occasion d'un recensement collectif auprès d'une population concernée dans la mesure où le comparaison a abouti à un résultat négatif ne sont pas insérés au traitement ADN criminalistique. Elle estime que tel devrait le cas et suggère de compléter le texte en ce sens et d'ajouter une disposition prescrivant la destruction de ces empreintes.

Il faudrait par ailleurs prévoir une disposition légale permettant à tout intéressé d'obtenir la radiation de ses propres données lorsque l'enquête pénale a établi la culpabilité d'un tiers et le coupable a été condamné en dernier ressort, ou encore mieux de prévoir un mécanisme, doté le cas échéant d'une alerte automatique, qui procède à la suppression des empreintes lorsque leur conservation n'apparaît plus nécessaire au regard de la finalité poursuivie.

Dans un souci d'éviter que des personnes innocentes restent fichées, le cas échéant même à leur insu ou contre leur volonté, en vue de comparaisons futures, le projet sous avis devrait clairement régler le sort de ces empreintes.

F) Articles 10 et 13 : la durée de conservation des profils ADN

Aux termes de l'article 10 paragraphe (1) du projet sous avis :

« Un profil d'ADN ayant pu être attribué à une personne déterminée ainsi que les informations y relatives peuvent faire l'objet du traitement ADN criminalistique jusqu'au jour où:

1. la personne à laquelle il se rapporte a été acquittée, par une décision judiciaire coulée en force de chose jugée, pour les faits ayant donné lieu à l'établissement de son profil d'ADN;

2. les faits ayant donné lieu à l'établissement du profil d'ADN en cause sont prescrits;

3. un délai de 10 ans s'est écoulé après le décès de cette personne. »

1) La Commission nationale se doit de souligner l'importance capitale de l'article 10 pour la protection de la vie privée des personnes concernées.

D'après le commentaire des articles, « les trois hypothèses visées par le paragraphe (1) de cet article poursuivent cependant un même but, à savoir celui de ne maintenir ces données dans le traitement ADN criminalistique qu'aussi longtemps que ce maintien est justifié par la finalité du traitement, conformément à l'esprit et à la lettre de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. » (cf. document parlementaire n° 5356/00, p. 22).

S'il est vrai que l'article en question passe sous silence si les données sont conservées de la façon la plus favorable pour la personne concernée, c'est-à-dire sont effacées dès l'instant où l'une des trois hypothèses se trouve remplie, ou si ce n'est qu'à compter du moment où la dernière des trois hypothèses se trouve réunie que l'effacement définitif des données est justifié, il n'en reste pas moins que seule la première interprétation consistant à supprimer les données du traitement ADN criminalistique dès que l'une des trois hypothèses se trouve remplie serait conforme avec le principe de finalité.

Pour souligner le caractère alternatif des trois hypothèses portant effacement des données du traitement ADN criminalistique, une précision afférente au niveau de l'article 10 paragraphe 1er s'impose dès lors et qui pourrait consister à ajouter à la fin de chaque hypothèse décrite le terme «ou».

2) Quant au premier point du premier paragraphe de l'article 10, il ressort du projet sous avis que seules les décisions judiciaires d'acquittement peuvent déclencher la suppression du profil d'ADN du traitement ADN criminalistique; que les décisions de classement sans suites, de condamnation avec sursis, probatoire ou non, ou encore de suspension du prononcé, probatoire ou non, sont sans influence sur le maintien du profil d'ADN en cause au traitement ADN criminalistique ; et que la même solution s'impose encore en cas de décision de non-lieu prononcée en application de l'article 128 du Code d'instruction criminelle alors qu'une reprise des poursuites reste possible s'il y a survenance de charges nouvelles au sens de l'article 135 du Code d'instruction criminelle. (cf. document parlementaire n° 5356/00, p. 22).

La Commission nationale voudrait exprimer ses plus grandes réserves par rapport à cette disposition du projet de loi, en particulier du maintien des données en cas de décisions de classement sans suites ou de non-lieu.

Elle estime que ces données ne sont plus pertinentes ni nécessaires au regard de la finalité poursuivie pour lesquelles elles ont été collectées et que leur conservation n'est dès lors plus justifié, de sorte que leur effacement est de mise conformément à l'article 4 paragraphe 1er de la loi du 2 août 2002.

La Commission nationale regrette que le projet sous avis ne comporte pas de disposition impérative en ce sens à l'instar de la législation française et renvoie à ce sujet à ses observations relatives au droit d'effacement.

3) En vertu de l'article 13 du projet sous avis, un profil d'ADN et les données à caractère personnel y afférentes ne peuvent plus faire l'objet du traitement ADN condamnés 10 ans après le décès de la personne à laquelle ces informations se rapportent.

Suivant le commentaire des articles, « la réhabilitation prévue par les articles 644 et suivants du Code d'instruction criminelle est sans influence sur le maintien des données ADN dans le traitement ADN criminalistique ».

D'abord, est-ce que les auteurs du projet sous avis n'ont-ils pas voulu viser ici le traitement ADN condamnés, et non pas le traitement ADN criminalistique tel que mentionné au commentaire des articles ?

Quoi qu'il en soit, la Commission nationale est d'avis qu'il n'y a plus de nécessité de faire figurer une personne réhabilitée dans le traitement criminalistique, voire condamnés, étant donné que la réhabilitation qui constitue un puissant instrument de resocialisation tend justement à permettre à l'ancien condamné de vivre dans des conditions et situations de nature à éviter de nouvelles manifestations criminelles ou délictueuses, prévues par le Code pénal (cf. document parlementaire, 1975-1976, n° 1718/01, cité dans « Lexique de procédure pénale de droit luxembourgeois », Gaston VOGEL, point 864, p. 347 et s.).

L'article 657 du code d'instruction criminelle dispose entre autres que la réhabilitation fait cesser pour l'avenir, dans la personne du condamné, tous les effets de la condamnation, sans préjudice des droits acquis aux tiers, notamment elle empêche que la condamnation serve de base à la récidive, fasse obstacle à la condamnation conditionnelle, ou soit mentionnée dans les extraits du casier judiciaire. L'article 658 du code d'instruction criminelle ajoute que les condamnations…seront effacées des registres du casier judiciaire lorsque la réhabilitation légale ou judiciaire sera acquise au condamné.

Concrètement, cela revient à dire que malgré le fait que le condamné a été réhabilité et ses condamnations enlevées des registres du casier judiciaire, les empreintes génétiques de cette personne restent dans le fichier ADN créé par le présent projet de loi.

Le traitement des données à caractère personnel relatives aux empreintes génétiques risque ainsi de devenir au fil du temps un casier judiciaire parallèle comportant des informations qui ne figurent pas au casier judiciaire lui-même.

4) Le second paragraphe de l'article 10 du projet de loi bouleverse de fond en comble le régime d'effacement instauré par le premier paragraphe en prévoyant le maintien de ces informations au traitement ADN criminalistique « si le profil d'ADN en cause a fait l'objet d'une comparaison positive en relation avec les faits d'une enquête préliminaire ou d'une instruction préparatoire ».

D'après le commentaire des articles, « le paragraphe (2) de cet article apporte un certain correctif au paragraphe (1) en ce qu'il vise à assurer que des données ADN peuvent être maintenues au traitement ADN criminalistique lorsque la finalité de ce traitement l'exige même si, stricto sensu, les hypothèses prévues par le paragraphe (1) se sont réalisées » au motif qu'il « ne faut pas oublier en effet que, d'une part, les profils d'ADN faisant l'objet du traitement ADN criminalistique ne sont pas exclusivement ceux de suspects, prévenus ou inculpés et que, d'autre part, une personne physique peut être impliquée dans plusieurs affaires en des qualités différentes, tantôt en tant qu'auteur, tantôt en tant que victime. » (cf. document parlementaire n° 5356/00, p. 22).

La Commission nationale reste perplexe quant au bien-fondé d'un pareil correctif qui peut engendrer des abus en pratique, puisque d'éventuels détournements de finalité se trouveront facilités.

5) La Commission nationale fait en outre siennes les réflexions de la Commission belge pour la protection de la vie privée exprimées dans son avis concernant l'avant-projet de loi relatif à l'analyse ADN en matière pénale en Belgique en ce qui concerne les objectifs recherchés par le législateur et sur la base de ceux-ci, les délais de conservation des profils ADN dans la banque de données "Criminalistique".

« Si l'objectif poursuivi par le législateur consiste uniquement à identifier des traces découvertes dans le cadre d'une infraction déterminée, cet objectif est atteint lorsque les traces ont été identifiées; les profils ADN devraient dès lors être effacés de la banque de données dès que l'identification a été réalisée. Dans cette optique, il conviendrait même de qualifier de disproportionné l'enregistrement de profils ADN déjà identifiés dans la banque de données "Criminalistique". Toutefois, si comme en l'espèce l'objectif est de disposer de suffisamment de moyens en vue d'enquêter sur des infractions futures, la conservation de traces identifiées peut se révéler importante. Dans ce cas, on crée toutefois une banque de données de suspects potentiels, avec toutes les possibilités d'abus que cela implique. (cf. avant-projet de loi relatif à l'analyse ADN en matière pénale ; Commission pour la protection de la vie privée, Belgique, Numéro : JZ985ED_1, Numéro de rôle : 17/98 du 14 mai 1998.)

Ainsi décidé à Esch-sur-Alzette en date du 8 octobre 2004

La Commission nationale pour la protection des données

(*s.*) Gérard Lommel	(*s.*) Edouard Delosch	(*s.*) Pierre Weimerskirch
Président	Membre effectif	Membre effectif

Avis de la Commission nationale pour la protection des données concernant le projet de règlement grand-ducal déterminant les services de communications électroniques et les services postaux ainsi que la nature, le format et les modalités de mise à disposition des données dans le cadre de l'article 41 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Délibération n° 84/2004 du 15 novembre 2004

La Commission nationale pour la protection des données (ci-après « la Commission nationale ») entend présenter ci-après ses observations et commentaires au sujet du projet de règlement grand-ducal déterminant les services de communications électroniques et les services postaux ainsi que la nature, le format et les modalités de mise à disposition des données dans le cadre de l'article 41 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel :

Article 1er :

La Commission nationale s'interroge sur le point de savoir si les services de communications électroniques et services postaux pour lesquels les opérateurs et fournisseurs de services doivent mettre à disposition les données conforme à l'article 41 paragraphe (2), ne devraient pas faire l'objet d'une première disposition du présent règlement grand-ducal.

Article 2 (1) :

- Le projet fait référence à « l'Institut » sans autre précision.

Pour une meilleure compréhension, ne serait-il pas préférable de préciser qu'il s'agit de l'Institut Luxembourgeois de Régulation, (ci-après « l'Institut »).

- Le texte de l'article ne précise pas par qui les données sont mises à disposition.

Pour une meilleure compréhension, il vaudrait mieux préciser les données … sont mises à disposition de l'Institut Luxembourgeois de Régulation, (ci-après « l'Institut ») par les opérateurs et fournisseurs de communications électroniques ainsi que des services postaux et des fournisseurs de ces services.

Article 4 :

- L'article 4 définit « le contenu des fichiers », c'est à dire la nature des données mises à disposition.
- Pour les données à mettre à disposition « en matière de services de communications électroniques », la Commission nationale fait remarquer que l'énumération des données sont celles relatives aux :

- services d'accès au réseau téléphonique public
- services téléphoniques accessibles au public
- services de transports de données
- services de messagerie électronique
- services Télex
- postes téléphoniques payant public

mais n'indique pas de façon claire de quelles données il s'agit.

- La Commission nationale s'interroge également si la mise à disposition des «données de localisation disponibles» ne dépasse pas le cadre tracé par l'article 41 paragraphe (1) de la loi.

En effet, cet article de la loi porte uniquement sur l'accès « aux données concernant l'identité des abonnés et des utilisateurs ».

Dans le projet de loi initial, il n'y avait pas de précision alors qu'il était question de transmettre « les données concernant les abonnés des opérateurs... ».

La précision est apparue dans l'amendement proposé par la Commission des Médias et des Communications, dans le document parlementaire n°4735/8, page 37 et commentée comme suit :

« (1) : L'amendement a pour objet de répondre aux inquiétudes exprimées par le Conseil d'Etat. L'accès a été limité aux autorités agissant dans le cadre des articles 88-1 à 88-4 du code d'instruction criminelle, dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du code d'instruction criminelle. La commission a également ajouté la centrale des secours d'urgence 112.

Ces autorités et centrale n'ont accès qu'aux données relatives à l'identité des abonnés et utilisateurs, à savoir nom, prénoms, adresse et, le cas échéant, l'adresse IP.

La centrale des secours d'urgence 112 n'a pas accès aux données des services postaux. La commission ne voit en effet pas l'utilité d'accès à ces données étant entendu que seule une situation d'urgence justifie une demande d'accès émanant de ladite centrale. »

La Commission nationale propose de modifier le texte de l'article 4, paragraphe (3) comme suit :

« les données à mettre à disposition par les opérateurs et fournisseurs de communications électroniques sont :

nom, prénoms, adresse et, le cas échéant, l'adresse IP de l'abonné et/ou de l'utilisateur des services suivants :

- Services d'accès au réseau téléphonique public,
- Services téléphoniques de transport de données
- Services de messagerie électronique
- Services Télex
- Postes téléphoniques payant publics

Ainsi que l'adresse du lieu où sont installés les postes et lignes fixes. »

Article 5 :

- Paragraphe (1) : il y lieu de compléter la phrase par la précision: « l'ensemble des fichiers énoncés à l'article 4 ».
- Paragraphe (2) : concernant les données de localisation, la Commission nationale renvoie à ses observations formulées à l'article 4.

Article 6 :

- Il est fait usage du terme « requérant initial » sans que ce terme ait au préalable fait l'objet d'une définition.
- La Commission nationale remarque encore qu'il est prévu de mettre à disposition des autorités compétentes visées par les articles 88-1 à 88-4 du Code d'instruction criminelle et les autorités agissant dans le cadre du crime ou délit flagrant « l'identité des opérateurs et fournisseurs de services respectifs »:

Ici encore, le projet de règlement grand-ducal ne dépasse-t-il pas également le cadre de l'article 41 de la loi qui prévoit seulement l'accès « aux données concernant l'identité des abonnés et utilisateurs… ».

De toute façon, en application de la loi il n'y a pas lieu de distinguer entre les données qui doivent être mises à disposition et les données transmises, alors que le paragraphe (2) de l'article 41 de la loi (concernant les données mises à disposition) renvoi au paragraphe (1er) de la loi (indiquant les données auquel l'accès est donné par l'Institut).

- La Commission nationale fait encore remarquer que les « données de localisation » au sens de la directive 2002/58 concernant notamment les téléphones portables ne seraient de toute façon pas exploitables dans la mesure où les données sont fournies à l'Institut « au moins une fois par jour par les fournisseurs et opérateurs ». Il en serait autrement si c'était l'Institut qui allait se renseigner à un moment déterminé, sur requête auprès des fournisseurs et opérateurs.

Article 8 :

- Paragraphe (1) :
  En vue de permettre le contrôle des accès et de la sécurité des données du système, nous recommandons d'ajouter la lettre (g) aux points énumérés (d) et (e) d'ores et déjà mentionnés.
- La Commission nationale fait encore remarquer que les données de traçage des accès au système devront lui être rendues accessibles en application de l'article 32 paragraphe (7) de la loi précitée du 2 août 2002.

Constat général :

Au vu des considérations exposées ci-dessus, la Commission nationale admet que dans certaines circonstances, il pourra être important pour la poursuite de l'enquête respectivement l'efficacité des secours d'urgences, que lesdites autorités aient connaissance des données de localisation disponibles ainsi que de l'identité des opérateurs et fournisseurs de services de ses abonnés et utilisateurs. Comme le texte de la loi ne prévoit actuellement pas ces aspects, il conviendrait d'élargir en ce sens l'article 41 de la loi.

Ainsi décidé à Esch-sur-Alzette en date du 15 novembre 2004.

Pour la Commission nationale pour la protection des données

(s.) Gérard Lommel	(s.) Edouard Delosch	(s.) Pierre Weimerskirch
Président	Membre effectif	Membre effectif

A propos de la licéité des tests de paternité

(Communiqué de presse)

A la suite du reportage diffusé sur RTL Télé Luxembourg le 16 janvier 2005, la Commission nationale pour la protection des données tient à faire la présente mise au point, afin d'éviter des malentendus éventuels quant à la licéité de la collecte et du traitement de données génétiques, en particulier en vue d'établir ou de vérifier une filiation par recoupement de séquences génétiques.

La législation luxembourgeoise comporte bel et bien des dispositions limitant le recours à des tests de paternité, et cela dans le cadre de l'article 6 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

En effet, dans l'hypothèse visée dans ledit reportage, la loi ne permet le traitement d'une telle donnée à caractère personnel, hautement sensible, que dans le cadre d'une procédure judiciaire.

Un test de paternité ne peut donc ni être demandé ni effectué à la simple demande d'un particulier, a fortiori si les données génétiques analysées ont été collectées à l'insu d'une des personnes concernées.

Esch-sur-Alzette, le 18 janvier 2005

Communiqué par la Commission nationale pour la protection des données

Commission Nationale pour la Protection des Données

Avis de la Commission nationale pour la protection des données concernant l'avant-projet de loi relatif à l'accès des officiers de police judiciaire à certains traitements de données à caractère personnel des personnes morales de droit public

Délibération n°66/2005 du 4 mai 2005

Conformément à l'article 32, paragraphe 3, lettre (e) de la loi 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 entre autres pour mission d'« être demandée en son avis sur 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, et faisant suite à la demande lui adressée par Monsieur le Ministre délégué aux Communications, que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet de l'avant-projet de loi relatif à l'accès des officiers de police judiciaire à certains traitements de données à caractère personnel des personnes morales de droit public.

I. Remarques préliminaires

A) La résurgence des attaques terroristes et le développement de réseaux internationaux de criminalité organisée suscite naturellement des mesures de la part des Etats démocratiques visant à renforcer la sécurité des citoyens face aux menaces qui s'amplifient à l'époque de la globalisation. L'Union européenne travaille à améliorer les moyens de collaboration policière et judiciaire et à faciliter les échanges de données personnelles nécessaires dans cette perspective. La tendance à faciliter l'accès des autorités chargées de la sécurité publique et de la sûreté de l'Etat aux fichiers publics et parfois à certains fichiers privés à suscité également des initiatives législatives nouvelles au niveau national et l'avant-projet de loi sous revue s'inscrit dans cette évolution.

Il est incontestable que la prévention, la constatation et la répression des infractions pénales constitue une finalité légitime pour de telles mesures dès lors qu'elles restent conformes aux principes de l'article 8 paragraphe 2 de la Convention européenne des Droits de l'Homme et qu'en particulier elles ne dépassent pas ce qui dans une société démocratique peut être considéré comme nécessaire pour assurer la sécurité publique, la prévention de la criminalité et la protection des droits et libertés d'autrui.

Il s'agit en revanche d'être vigilant afin de contribuer à ce que les mesures nouvelles ne prennent des proportions excessives ou dépassent ce qui est nécessaire dans les Etats démocratiques pour satisfaire les besoins correspondant à la finalité légitime de protection de la sécurité des citoyens et des Etats eux-mêmes.

En d'autres termes une certaine modération apparaît de mise dans cette démarche afin d'éviter que dans le but de protéger la démocratie, les libertés et droits fondamentaux ne soient affectés de façon telle que c'est la démocratie elle-même qui se retrouve affaiblie par les mesures censées la protéger.

B) Aux termes de l'article 3 paragraphe (3) de la loi du 2 août 2002 ladite loi-cadre s'applique aux traitements de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, même liées à un intérêt économique ou financier important de l'Etat, sans préjudice des dispositions spécifiques de droit national ou international régissant ces domaines.

Comme il ressort de l'exposé des motifs (document parlementaire 4735/00, p. 83), le législateur a en effet opté pour un champ d'application large qui s'étend également aux personnes morales ainsi qu'aux personnes publiques, aux domaines de la défense, de la sécurité publique et de la sûreté de l'Etat ainsi qu'aux activités liées au droit pénal en vue d'instaurer un régime juridique unifié capable d'offrir un niveau de sécurité juridique approprié aux personnes concernées.

L'inclusion des quatre matières susvisées (méthode adoptée par la loi portugaise et en partie par la loi belge) est permise par la Directive 95/46/CE (du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) et présente les avantages suivants :

- clarification et unification du régime juridique de la protection des données tout en autorisant à l'Etat de prévoir les limitations et dérogations nécessaires à l'exercice de la puissance publique. Certaines limitations et dérogations sont d'ores et déjà comprises dans le projet de loi. … Les limitations et dérogations prévues par les lois actuellement en vigueur joueront entièrement, dès lors qu'elles touchent aux personnes morales, à la défense, la sécurité publique, la sûreté et aux activités liées au droit pénal. De plus, des lois spéciales pourront à l'avenir édicter de telles limitations et dérogations.
- modifications légères des règlements grand-ducaux existants en la matière …

Les principes du droit relatif à la protection des données s'appliquent donc en règle générale également dans les quatre matières susvisées.

C) Afin de situer les observations de la Commission nationale pour la protection des données dans le contexte légal approprié, il paraît également indiqué de rappeler d'emblée la teneur de l'article 8 de la Convention européenne des Droits de l'Homme (CEDH) intitulé « Droit au respect de la vie privée et familiale » qui dispose que :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

Il en découle que la protection de la vie privée est la règle, et que l'ingérence dans l'exercice de ce droit doit rester l'exception.

La Commission nationale ne saurait donc approuver l'introduction de dérogations nouvelles au principe de la protection de la vie privée par l'avant-projet de loi sous avis dès lors que le juste équilibre entre le principe et les exceptions reste préservé.

D) Rappelons aussi la jurisprudence de la Cour européenne des droits de l'homme selon laquelle l'enregistrement et la conservation a priori des données ne peut en aucun cas mener à des mesures de surveillance exploratoires ou générales (Arrêts Klass (arrêt du 6 septembre 1978, Publ. Cour, Série A, n° 28, p. 23 et s) et Malone).

« La Cour souligne néanmoins que les Etats contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée. » (cf. arrêt Klass et autres du 6 septembre 1978, série A n° 28, pp. 23-24, paras. 49-50) ;

« Néanmoins, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendre » (cf. arrêt Leander, n° 10/1985/96/144, du 25 février 1987, point 60).

E) Il est intéressant de relever à cet égard que la Cour de Justice des Communautés Européennes a, elle aussi, dans un arrêt récent du 20 mai 2003, soumis le contrôle de la compatibilité de la réglementation nationale (en l'occurrence autrichienne) avec les dispositions de la directive (95/46/CE) à une vérification préalable de sa compatibilité avec l'article 8 de la Convention européenne des droits de l'homme (CEDH) sur la protection de la vie privée en soulignant que la communication, par l'employeur à un tiers, de données relatives aux revenus perçus par un travailleur ou un pensionné est une ingérence dans la vie privée au sens de l'article 8 de la CEDH qui ne peut être justifiée que si elle est prévue par la loi, poursuit un but légitime visé dans cet article et est nécessaire dans une société démocratique pour atteindre ce but (cf. Affaires jointes C-465/00, C-138/01 et C-139/01 - Rechnungshof (C-465/00) contre Österreichischer Rundfunk et autres et Christa Neukomm (C-138/01) et Joseph Lauermann (C-139/01) contre Österreichischer Rundfunk).

La marge de manœuvre du législateur se trouve donc enfermée dans les limites posées par l'article 8 paragraphe 2 de la CEDH.

F) La Commission nationale aimerait dans ce contexte encore relever le « rapport sur l'incidence des principes de la protection des données sur les données judiciaires en matière pénale y compris dans le cadre de la coopération judiciaire en matière pénale », qui prévoit plus particulièrement sous les points 10 et 54 :

« 10. En vertu de l'article 3 de la Convention 108 : « Les Parties s'engagent à appliquer la présente Convention aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé ». Le champ d'application de la Convention devrait donc en principe englober les données à caractère personnel relatives à des individus impliqués dans une procédure judiciaire et soumises à des traitements automatisés par le système judiciaire si les Parties à la Convention n'ont pas exclu ces catégories de fichiers automatisés à caractère personnel du champ d'application de la Convention, en conformité avec l'article 3, paragraphe 2, alinéa a, de la Convention 108. En outre, la Convention 108 peut aussi s'appliquer aux données judiciaires à caractère personnel ne faisant pas l'objet de traitements automatisés, pour peu que les Parties aient fait la déclaration mentionnée à l'article 3, paragraphe 2, alinéa c.

54. Des autorités nationales de contrôle de la protection des données ont été mises en place dans la quasi-totalité des pays d'Europe. Elles jouissent de compétences leur permettant d'assurer le respect et l'intégration au droit interne des principes énoncés dans la Convention 108 ainsi que des dispositions de la législation nationale en matière de la protection des données. Elles sont par conséquent également habilitées à surveiller, contrôler et vérifier l'application de ces principes dans différents secteurs. Néanmoins, dans certains pays, des autorités indépendantes de contrôle de la protection des données ont été mises en place pour contrôler les échanges d'information entre les autorités judiciaires et le traitement des données par ces mêmes autorités. Dans ces pays, on a considéré, d'une part, que les autorités de contrôle de la protection des données n'avaient en général aucune compétence juridictionnelle et que le principe de la séparation des pouvoirs législatif, exécutif et judiciaire ne permettait pas le contrôle des activités du pouvoir judiciaire. D'autre part, comme les autorités judiciaires collectent et traitent elles-mêmes des données à caractère personnel, il est apparu que ceci pouvait également être soumis à un contrôle des autorités de contrôle de la protection des données. La Convention 108 et son protocole additionnel s'appliquent aux données à caractère personnel concernant les personnes impliquées dans une procédure judiciaire et qui sont traitées par les services judiciaires, sauf dans le cas où les Parties à ces instruments internationaux ont fait une déclaration excluant explicitement ces catégories de données de leur champ d'application, conformément à l'article 3.2.a de la Convention 108. »

(http://www.coe.int/T/F/Affaires_juridiques/Coop%E9ration_juridique/Protection_des_donn%E9es/Documents/Rapports/R-Report%20on%20police%20and%20judicial%20data%20f%20090403.asp#TopOfPage

Force est de constater que les réserves formulées par le Grand-Duché de Luxembourg au titre de l'article 3.2. a) de la Convention 108 dans la loi du 19 novembre 1987 portant approbation de la cette convention ne visent pas les traitements de données judiciaires, de sorte qu'il faut en conclure que les principes y arrêtés devraient s'appliquer aux données judiciaires.

En effet, l'article 2 de la loi précitée du 19 novembre 1987 dispose que :

« Le Grand-Duché de Luxembourg déclare qu'il se réserve le droit, dans les limites de l'article 3 (2) de la Convention, de ne pas appliquer la Convention

a) aux banques de données qui en vertu d'une loi ou d'un règlement sont accessibles au public ;

b) à celles qui contiennent exclusivement des données en rapport avec le propriétaire de la banque ;

c) à celles qui sont établies pour compte des institutions de droit international public. »

II. Articles 24-1 et 67-2 nouveaux

A) Un champ d'application très vaste

Aux termes de l'article 24-1 nouveau du code d'instruction criminelle, ce nouveau droit d'accès par voie informatique aux données d'autres personnes morales de droit public à instaurer au bénéfice du Procureur d'Etat et des officiers de police judiciaire agissant sur son instruction aura une portée très étendue, alors que l'article sous commentaire vise indistinctement tous les administrations et services de l'Etat ainsi que tous les établissements publics. Il en est de même en ce qui concerne le juge d'instruction et des officiers de police judiciaire agissant sur commission rogatoire au vœu de l'article 67-2 nouveau du code d'instruction criminelle.

Les articles 24-1 et 67-2 nouveaux à insérer au code d'instruction criminelle (article 1er de l'avant-projet de loi sous avis) visent donc à assurer au procureur d'Etat, aux officiers de police judiciaire (ci-après dénommés en abrégé OPJ) ainsi qu'au juge d'instruction l'accès à toutes données figurant dans des fichiers des personnes morales de droit public, sauf les quelques exceptions prévues par l'avant-projet de loi sous avis.

Tomberaient donc dans le champ d'application des nouvelles dispositions des traitements de données comme ceux opérés par les établissements publics industriels et commerciaux, tels que l'Entreprise des Postes et Télécommunications, la Banque et Caisse d'Epargne de l'Etat ou le Centre thermal de Mondorf-les-Bains.

La Commission nationale estime en revanche qu'il y aurait lieu de limiter la portée des nouvelles dispositions aux fichiers détenus par les personnes morales de droit public comme l'Etat, les communes, les syndicats de communes, les établissements publics administratifs et autres administrations ou services relevant de ces personnes morales ayant pour mission l'exécution d'un service public administratif, à l'exception des entités poursuivant une activité économique ou commerciale, telles que les établissements publics industriels ou commerciaux (cf. Instruction du Gouvernement en conseil du 11 juin 2004 ayant pour objet de fixer une ligne de conduite et des règles générales en matière de création d'établissements publics et retenant la qualification soit d'un établissement public à caractère administratif (EPA), soit d'un établissement public à caractère industriel et commercial (EPIC), soit d'un établissement public à caractère culturel, social et scientifique (EPCSS), à tout établissement à créer).

Dans la mesure où l'intention des auteurs du projet consiste à limiter l'accès à des fichiers détenus - ou à des traitements de données opérés - par des services publics administratifs exerçant une mission d'intérêt général, il faudrait expressément exclure du champ d'application envisagé les personnes de droit public exerçant en tout ou en partie une activité économique.

Il convient en effet d'avoir à l'esprit qu'un accès direct de façon horizontale à un nombre impressionnant de fichiers des différents organismes publics et les moyens informatiques d'exploiter les données sont susceptibles de comporter des risques de non-respect des principes de proportionnalité et de finalité.

B) Une nouvelle forme de perquisition « perquisition électronique »

D'après le commentaire des articles, la formulation « accès par un système informatique direct » « est inspirée du nouvel article 60-1 du code de procédure pénale français ».

A la lecture dudit article 60-1, il appert cependant que tant sa signification que sa portée sont différentes de celles que l'on veut lui conférer.

Il est intéressant de rappeler que le nouvel article 60-1 du code de procédure pénale français a été introduit par une loi (2003-239) du 18 mars 2003 dite « Loi pour la sécurité intérieure », dont les dispositions les plus pertinentes pour le présent avis sont les suivantes :

« Chapitre IV - Dispositions relatives aux investigations judiciaires

(...)

Article 17

Le code de procédure pénale est ainsi modifié :

1° Après l'article 57, il est inséré un article 57-1 ainsi rédigé :

« Art. 57-1. - Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

« S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.

« Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support. Les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code. » ;

(...)Article 18

Le code de procédure pénale est ainsi modifié :

1° Il est inséré, après l'article 60, un article 60-1 ainsi rédigé :

« Art. 60-1. - Sur demande de l'officier de police judiciaire, qui peut intervenir par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé, à l'exception de ceux visés au deuxième alinéa de l'article 31 et à l'article 33 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.

« L'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés à l'article 43-7 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs.

« Les organismes ou personnes visés au présent article mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais.

« Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni d'une amende de 3 750 EUR. Les personnes morales peuvent être déclarées responsables pénalement dans les conditions prévues par l'article 121-2 du code pénal de l'infraction prévue au présent alinéa. La peine encourue par les personnes morales est l'amende, suivant les modalités prévues par l'article 131-38 du code pénal.

« Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les catégories d'organismes visés au premier alinéa ainsi que les modalités d'interrogation, de transmission et de traitement des informations requises. ».

Force est de constater que le projet luxembourgeois entend accorder des pouvoirs exorbitants à différents acteurs du monde judiciaire et policier qui dépassent de loin les prérogatives que le législateur français a accordé aux mêmes organes à travers les articles 57-1 et 60-1 précités.

En effet, le projet sous avis instaure un accès direct par voie informatique à l'initiative des forces de l'ordre, du Procureur d'Etat et du juge d'instruction qui n'est nullement prévu par les dispositions légales françaises pour lesquelles l'officier de police judiciaire doit faire une demande expresse (cette demande pouvant intervenir par voie informatique).

Dans ce contexte, la Commission nationale aimerait encore relever que, d'après ses informations, une telle procédure d'accès facilitant les techniques comme le matching et le datawarehouse (c'est-à-dire la comparaison de données à partir de deux fichiers afin de déceler des différences), ne serait guère concevable en Allemagne, pays soucieux de préserver au maximum le strict cloisonnement des banques de données détenues par les différentes administrations publiques.

Contrairement au texte français qui prévoit une stricte séparation des fichiers des organismes publics non accessibles directement par l'extérieur, le texte luxembourgeois sous avis permet ainsi aux acteurs susmentionnés, sans requérir le consentement du responsable du traitement dudit fichier, de consulter des données traitées par autrui.

Cette interprétation du texte est corroborée par le terme « système informatique direct », le terme « direct » semble a priori être en contradiction avec l'optique du législateur français prévoyant la notification d'une demande préalable à l'organisme public.

La Commission nationale est dès lors d'avis qu'il vaudrait mieux se limiter à la logique adoptée par la loi française qui instaure en quelque sorte une forme de « perquisition électronique » adoucie dans laquelle l'OPJ bénéficie d'un « push » de la part de l'administration publique, mais non d'un « pull », c'est-à-dire d'un accès par système informatique direct, tel que retenu dans l'avant-projet de loi sous avis.

L'initiative législative se trouvant cantonnée et circonscrite par l'article 8 de la CEDH, il convient d'entourer la nouvelle forme envisagée de perquisition de garanties suffisantes, à l'instar des conditions strictes prévues par le Code d'instruction criminelle pour la perquisition « classique » qui ne permettent pas le recours à des perquisitions clandestines, c'est-à-dire effectuées à l'insu de la personne concernée, où se pose le cas échéant un problème des droits de la défense.

C) Le rôle du responsable du traitement initial

Il faut se demander si cet accès direct par un tiers n'est pas contraire aux responsabilités attachées à la notion de « responsable du traitement » dans le droit de la protection des données.

L'importance du rôle primordial joué par le responsable du traitement peut être retrouvée à l'article 2 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (adoptée par le Conseil de l'Europe à Strasbourg le 28 janvier 1981) qui définit à la lettre d) le «maître du fichier» comme étant « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées ».

En cas d'utilisation illicite de données à caractère personnel, c'est le maître du fichier, le responsable du traitement, qui voit sa responsabilité engagée en premier lieu, qu'elle soit de nature civile, pénale ou administrative. Il devrait donc conserver la maîtrise sur ses données au lieu de les voir passivement accédées de l'extérieur.

D) La fragilisation des règles relatives à la confidentialité et à la sécurité des données

Dans le même ordre d'idée, l'on peut s'interroger si une telle solution ne pose pas problème en termes de confidentialité des données et de sécurité des traitements au sens des articles 21, 22, 23 et 25 de la loi du 2 août 2002. Cette personne de droit public sera-t-elle toujours en mesure de respecter les exigences afférentes posées par la loi si un accès direct est réservé à un tiers, en l'occurrence les forces de l'ordre ou le Procureur d'Etat ?

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 collectées ou obtenues. En particulier il doit s'en assurer lorsqu'il communique ces données à des destinataires y compris des sous-traitants 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 protection des données et la sécurité des traitements.

Au regard de la définition donnée à l'article 2 lettre (s) du terme « traitement », la loi du 2 août 2002 ne prévoit que « la communication par transmission, la diffusion ou toute autre forme de mise à disposition » comme opérations appliquées à des données à caractère personnel. S'agissant d'un « push » effectué par le responsable du traitement, ces opérations constituent des modes de transmission actifs, par opposition au « pull » prévu au projet sous avis qui constitue un mode de transmission où le responsable du traitement reste passif.

Le responsable du traitement étant en quelque sorte gardien et des données et de la compatibilité des finalités des traitements, il doit aussi veiller à ce que la communication des données à caractère personnel à un tiers se fasse selon le même principe de finalité et soit compatible avec le traitement initial.

L'optique de responsabilisation empruntée par la loi du 2 août 2002 ne paraît donc guère conciliable avec le cas de figure envisagé où des données à caractère personnel pourraient être accédées, extraites, copiées par des tiers -fussent-ils les autorités judiciaires et policières dans le cadre de l'exercice de leurs missions légales- à l'insu du titulaire de ladite responsabilité (gardien de la sécurité des données et de leur utilisation loyale) qui ne pourrait plus, sinon difficilement, l'assumer.

A l'instar de l'article 4 paragraphe 2 in fine de la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat, la Commission nationale se demande dès lors s'il ne paraît pas indiqué d'imposer l'obligation de consigner dans des fichiers de traçage (loggings) les accès opérés et les fichiers consultés.

E) L'exclusion des données protégées par un secret prévu par la loi

Il se pose encore la question de la praticabilité de l'exception inscrite dans le texte prévoyant que ne sont pas accessibles les données protégées par un secret prévu par la loi (ex : secret médical, fiscal ou bancaire).

Contrairement à la situation française où l'organisme public reste maître de la sélection des informations à mettre à disposition de l'officier de police judiciaire en fonction du critère légal « données soumis (ou non) à un secret prévu par la loi », le projet sous avis (ayant adoptée une approche différente) ne règle pas cette question.

Or, la Commission nationale s'interroge de quelle façon il pourra être garanti que resteront exclues de l'accès les données couvertes par un secret prévu par la loi.

L'option retenue du « ont accès par un système informatique direct » semble inappropriée, parce que l'accès se fera sans la personne morale de droit public liée par un secret professionnel.

Si la décision d'apprécier le caractère de confidentialité incombe à la police, au parquet ou au juge d'instruction le secret professionnel sera violé dans la mesure où l'analyse concrète des données collectées révèle leur caractère confidentiel.

Les considérations qui précèdent plaident en faveur de l'adoption d'une procédure similaire à celle inscrite dans la loi française.

La Commission nationale ne saurait soutenir une approche dans laquelle l'organisme public resterait passif, alors qu'il incombe à chaque établissement de communiquer, après avoir apprécié la légalité (dont le secret professionnel) de la demande lui adressée, quelles données doivent être communiquées à la police, au parquet ou au juge d'instruction.

III) Recommandation d'introduire un système technique « black box » au niveau des articles 41-1 et 17-1 nouveaux : une solution technique plus respectueuse de la vie privée

A) Au niveau des articles 41-1 et 17-1 nouveaux de l'avant-projet de loi sous avis, la Commission nationale exige l'introduction d'un système technique dit « black box » en suggérant au législateur d'adopter la même solution d'ores et déjà retenue à l'article 41 de la loi de la loi du 2 août 2002.

En effet, la voie très prudente empruntée par le législateur dans le cadre de l'article 41 de la loi est beaucoup plus protectrice des intérêts des personnes concernées en termes de confidentialité des données et sécurité des traitements que celle envisagée à l'article 41-1 nouveau de l'avant-projet de loi sous avis au profit de la police grand-ducale et de l'Inspection générale de la police dans l'exercice de leurs missions de police administrative, alors qu'en vertu du paragraphe 4 de l'article 41 (4) « la procédure est entièrement automatisée suite à l'autorisation de la Commission nationale. La Commission nationale vérifiera en particulier la sécurisation du système informatique utilisé. Cette automatisation permettra l'accès à distance par voie de communication électronique. »

Si le législateur retient, pour des raisons de protection de la vie privée, une solution technique très sophistiquée pour les seules données concernant l'identité des abonnés en vertu de l'article 41 de la loi, la Commission nationale estime qu' il devrait, a fortiori, en faire de même au niveau de l'article 41-1 nouveau pour des données à caractère personnel d'autant plus sensibles détenues par des personnes morales de droit public.

B) Pour les mêmes motifs, l'article 17-1 devrait également, à son tour, faire un renvoi à l'article 41-1 nouveau qui détaillerait les modalités techniques en s'inspirant de l'article 41 actuel de la loi où la procédure est décrite.

C) La Commission nationale relève que les auteurs de l'avant-projet sous avis se sont inspirés dans une très large mesure de la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat, dont le projet de loi afférent n'a pas été soumis à l'époque pour avis à la Commission nationale, qui prévoit en son article 4 :

« Art. 4. – Accès aux informations

(1) Le traitement, par le Service de Renseignement, des informations collectées dans le cadre de sa mission est mis en œuvre par voie de règlement grand-ducal tel que prévu par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

(2) Dans le cadre de l'exercice de sa mission, le Service de Renseignement est autorisé à accéder aux banques de données suivantes:

a. le registre général des personnes physiques et morales créé par la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales;

b. la partie „recherche" de la banque de données nominatives de police générale;

c. le bulletin N° 2 du casier judiciaire;

d. la banque de données des étrangers exploitée pour le compte du service de la police des étrangers au ministère de la Justice;

e. la banque de données relatives aux affiliations des salariés, des indépendants et des employeurs gérée par le centre commun de la sécurité sociale sur la base de l'article 321 du Code des assurances sociales;

f. la banque de données des véhicules routiers et de leurs propriétaires et détenteurs exploitée pour le compte du ministère des Transports.

L'accès à ces banques de données est soumis à la surveillance de l'autorité de contrôle visée à l'article 17, paragraphe (2) 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 vue de la surveillance exercée par cette autorité de contrôle, le Service de Renseignement doit mettre en œuvre les moyens techniques permettant de garantir le caractère retraçable de l'accès.

(3) Les données recueillies par le Service de Renseignement ne peuvent servir qu'à la réalisation des missions déterminées à l'article 2.

(4) Le Service de Renseignement peut solliciter les données à caractère non personnel nécessaires à l'exercice de ses missions auprès des personnes morales de droit public ou de droit privé et de toutes personnes physiques. »

La Commission nationale suggère de prévoir aussi dans le présent avant-projet de loi un tel système de traçage, qui est nécessaire de surcroît en vue d'assurer l'efficacité du contrôle exercé conformément à l'article 17-1 paragraphe 4 nouveau.

D) La Commission nationale est en outre d'avis qu'il vaudrait mieux supprimer dans l'article 17-1 paragraphe 2 nouveau la référence « ou, en cas d'urgence dûment motivée, au contrôle de l'existence des éléments constitutifs d'une infraction pénale », alors qu'il s'agit d'un critère de délimitation à la fois vaste et vague et que la mise en place d'un système de black box n'est guère concevable, voire praticable, avec une telle foule d'informations à gérer.

En effet, à la lecture de l'avant-projet de loi sous avis, plusieurs questions restent ouvertes :

- Qui apprécie le cas d'urgence et la motivation y relative ?
- Quelles infractions pénales (crimes, délits, contraventions) sont visées ?
- Quelles données à caractère personnel sont effectivement collectées et traitées ?
- Est-ce que ces données à caractère personnel ne varient-elles pas en fonction de la personne morale de droit public concernée ?

La Commission nationale estime dès lors qu'il faudrait prévoir une nomenclature précise des données consultées par rapport à chaque organisme public en procédant à une énumération limitative par fichier public, étant donné que les catégories de données recensées seront différentes d'une administration à l'autre.

A titre d'exemple, au niveau du Centre Commun de la Sécurité Sociale, il apparaît que les données relatives à l'employeur actuel, aux employeurs précédents ainsi qu'aux périodes d'affiliation devraient être suffisantes.

E) De façon générale, un autre point qui mériterait d'être clarifié dans ce contexte est celui de savoir ce qu'il faut entendre par « Peuvent seulement être obtenues les données qui sont nécessaires à l'identification des personnes physiques ou morales… » (cf. art. 17-1 paragraphe 2 nouveau ; art. 41-1 paragraphe 2 nouveau). Qu'est-ce que cela signifie au juste ? S'agit-il simplement de vérifier l'identité de la personne concernée par comparaison avec les informations détenues par les personnes morales de droit public ? L'exposé des motifs ne fournit point de précisions à cet égard.

F) Par ailleurs, l'avant-projet de loi sous avis passe également sous silence la durée de conservation des données ainsi consultées, durée qui doit être proportionnée aux finalités poursuivies conformément à l'article 4 paragraphe 1er lettre d) de la loi du 2 août 2002.

IV) Quant à l'article 17-2 nouveau relatif au traitement de données « douces » et « ultra douces »

L'exposé des motifs est muet quant à l'objectif recherché par l'introduction de l'article 17-2 dans la loi du 2 août 2002 qui, suivant la lettre d'accompagnement du ministre de tutelle, concerne le traitement de données « douces » et « ultra douces ».

A défaut d'explications afférentes, la Commission nationale limite ses commentaires à quelques réflexions d'ordre général :

A) La Commission nationale constate que les données à caractère personnel traitées au titre du nouvel article 17-2 ont été pour l'essentiel reprises des articles 8, paragraphe 1er et 10, paragraphe 1er de la Convention EUROPOL du 18 juillet 1995, de sorte qu'elle n'a pas d'observations particulières à présenter au sujet des données ou catégories de données contenues dans l'avant-projet de loi sous avis, tout en rappelant le caractère extrêmement sensible de ces traitements.

B) Si l'intention des auteurs de l'avant-projet de loi consistant à faire inscrire de telles dispositions dans une loi est louable en tant que telle, les garanties appropriées qui doivent les entourer ne doivent pas être amoindries pour ce type de traitement de données.

La Commission nationale estime dès lors qu'il faut également au niveau de cette disposition légale limiter l'usage et l'accès aux données aux seuls officiers de police judiciaire, comme prévu par les autres dispositions de l'avant-projet de loi sous avis.

C) Par ailleurs, il conviendrait de soumettre explicitement le traitement des données à caractère personnel énumérées à l'article 17-2 nouveau à la surveillance de l'autorité de contrôle prévue à l'article 17 de la loi du 2 août 2002.

Dans un souci d'assurer le parallélisme avec le paragraphe 4 de l'article 17-1 nouveau prévoyant expressément une surveillance de la part de l'autorité de contrôle prévue à l'article 17 de la loi, la Commission nationale recommande d'insérer le même paragraphe 4 également à l'article 17-2 de l'avant-projet de loi sous avis.

D) 1) Si l'intention des auteurs de l'avant-projet est celle de régler par la voie législative, plutôt que réglementaire, le traitement de données « douces » et « ultra douces » par les organes du corps de la police grand-ducale, de l'Inspection générale de la police et de l'administration des douanes et accises, cette approche est en tant que telle louable, mais devrait aller de pair avec le souci d'instaurer des garanties appropriées au niveau du texte légal, à l'instar de l'actuel article 17 qui prévoit (en son paragraphe 1er lettre a)) à ce sujet que l'autorisation par voie réglementaire « déterminera le responsable du traitement, la condition de légitimité du traitement, la ou les finalités du traitement, la ou les catégories de personnes concernées et les données ou les catégories de données s'y rapportant, l'origine de ces données, les tiers ou les catégories de tiers auxquels ces données peuvent être communiquées et les mesures à prendre pour assurer la sécurité du traitement en application de l'article 22 de la présente loi ».

Ces précisions sont nécessaires pour respecter les principes de base prévus à l'article 4 de la loi du 2 août 2002, à savoir les principes de licéité, de finalité, de transparence et de proportionnalité.

2) S'il est vrai que l'article sous avis permet de retenir comme condition de légitimité celle tirée de l'article 5 (1) (a) de la loi du 2 août 2002 prévoyant que le traitement de données peut être effectué lorsqu'il est « nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique » et que les finalités ont également été indiquées avec une précision suffisante « aux fins de la prévention, de la recherche et de la constatation des infractions pénales », il n'en reste pas moins que dans l'avant-projet de loi sous avis omet de mentionner les catégories de destinataires et la durée de conservation des données.

La Commission nationale estime que l'avant-projet de loi sous avis devrait expressément exclure toute communication à un tiers.

Quant à la durée de stockage, elle recommande de se référer aux principes dégagés (voir document cité ci-après du Conseil de l'Europe), sinon pour le moins rappeler les règles générales ancrées dans l'article 4 de la loi du 2 août 2002.

En outre, l'avant-projet de loi sous avis devrait clairement préciser les mesures organisationnelles et techniques à prendre pour assurer la confidentialité et la sécurité du traitement en application des articles 21 à 23 de la loi du 2 août 2002.

3) Dans le présent contexte, la Commission nationale aimerait attirer l'attention sur deux documents élaborés au niveau du Conseil de l'Europe :

a) Aux termes de l'article 14 du rapport sur la troisième évaluation de la Recommandation N° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, faite en 2002 :

http://www.coe.int/T/F/Affaires_juridiques/Coop%E9ration_juridique/Protection_des_donn%E9es/Documents/Rapports/Z-Rapport%203e%20EvalRec%20%2887%2915.asp#TopOfPage

14. Le CJ-PD a également convenu que les deux types de fichiers – permanents et ad hoc – pouvaient contenir des « informations criminelles » (parfois appelées « données douces »), qui sont des données non vérifiées et dont le lien avec les objectifs de la police doit être établi. Les données de ce type, qui donnent des indications non confirmées ou font naître des soupçons sur la participation d'une personne à une ou plusieurs infractions pénales, peuvent poser des problèmes du point de vue de la protection des données car elles peuvent être traitées à des fins différentes, voire à des fins générales de prévention, même si elles ne sont ni suffisantes ni exactes. Ces informations criminelles, en tant que phénomène nouveau non spécifiquement traité dans la Recommandation n° R(87)15, ont fait l'objet d'un examen dans le rapport de la deuxième évaluation de cette Recommandation, et certaines propositions ont été faites (voir document CJ-PD(2002)01). L'autre type de données contenues dans les fichiers permanents et ad hoc sont les données dites « solides », qui ont déjà été vérifiées. La principale différence entre ces « données solides » et les « informations criminelles » ou « données vagues » est le degré d'exactitude ou de fiabilité (à cet égard voir le Principe 2, paragraphe 2 de la Recommandation n° R(87)15).

b) Aux termes de l'article 5 de la deuxième évaluation de la pertinence de la Recommandation N°R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, faite en 1998.

(http://www.coe.int/T/F/Affaires_juridiques/Coop%E9ration_juridique/Protection_des_donn%E9es/Documents/Rapports/Y-Rapport%202e%20EvalRec%2887%2915.asp#TopOfPage)

5. Informations en matière criminelle

5.1 Portée du concept d'information criminelle

Un phénomène nouveau, qui n'est pas spécifiquement traité dans la Recommandation R(87) 15, est celui d'information en matière criminelle. Cette expression n'est pas dénuée d'ambiguïté. On peut établir plusieurs distinctions.

a. Les données «solides» et les données «vagues». Les données de police concernant des délinquants peuvent être (1) des données provenant de sources attestées ou (2) des données fondées sur de très vagues indications concernant l'implication éventuelle d'une personne dans le crime organisé. Nous qualifierons les premières de données «solides», les secondes de données «vagues». Ces dernières données peuvent même provenir d'une source anonyme dont la fiabilité est totalement incertaine. La nature de l'information peut néanmoins être telle que l'on peut juger le stockage nécessaire pendant une période limitée, afin que la police puisse travailler correctement.

b. Les données sur les personnes suspectées d'avoir commis une infraction spécifique ou sur lesquelles certaines indications permettent de penser qu'elles en commettent ou en préparent une, seules ou dans le cadre d'une organisation. Les pouvoirs de la police et de la justice étant limités dans la plupart des codes de procédure pénale aux cas où il y a suspicion à l'égard d'une personne concernant une infraction spécifique, les nouvelles technologies de l'information servent de plus en plus à stocker des données sur les délinquants en tant que personnes, sans relation avec telle ou telle infraction. Ces données peuvent être «vagues» ou «solides» comme expliqué plus haut. Elles n'ont pas forcément la valeur d'une forte présomption à l'encontre d'une personne, condition nécessaire à l'exercice des pouvoirs que le code de procédure pénale confère à la police. Néanmoins, de nombreux pays collectent de telles données, sur la base desquelles il arrive que l'on établisse un profil du criminel supposé (comportement, fréquentations, mode de vie) sans que ces recherches aient vraiment un rapport avec une infraction particulière. Ces données sont utilisées pour tout type de délit, qu'il soit déjà commis ou que l'on s'attende à ce qu'il le soit. Elles ne servent pas uniquement dans le cadre de l'enquête, ni comme élément de preuve dans une affaire pénale donnée. Tant qu'aucune règle précise n'est prévue dans le code de procédure pénale ou dans le droit (régional) de la police, ces données sont régies par les principes généraux s'appliquant à la protection des données. Pour les besoins du présent document, l'expression «informations en matière criminelle» sera utilisée dans ce deuxième sens.

Autrement dit, les données ne sont pas considérées comme des «informations en matière criminelle» si elles sont recueillies dans le cadre d'une enquête judiciaire et qu'il existe des raisons plausibles de soupçonner une personne d'avoir commis une infraction pénale donnée, indépendamment du fait de savoir si :

(1) ces données ne servent que dans le cadre de l'instruction d'une affaire particulière ou si elles serviront éventuellement plus tard dans des enquêtes sur d'autres infractions;

(2) ces données ont été recueillies dans le cadre ou non des pouvoirs accordés par le code de procédure pénale.

Dans certains pays, de telles données ne peuvent être retenues comme éléments de preuve lors d'un procès. Elles ne servent qu'à guider l'enquête de la police, mais peuvent toutefois devenir pertinentes au cours d'un jugement si la défense met en cause la manière dont les moyens de preuve ont été recueillis. On peut alors contester la légalité de leur stockage, car les moyens de preuve en question sont viciés au départ.

5.2 Question concernant les informations en matière criminelle

S'agissant de la collecte et du stockage d'informations en matière criminelle, il convient de répondre à plusieurs questions.

5.2.1 Qui peut faire l'objet d'informations en matière criminelle ?

Le droit au respect de la vie privée implique que ces informations ne peuvent concerner indifféremment toute personne ; la loi doit donc définir les critères permettant de définir les "cibles" potentielles de telles informations. Ces critères seront variables selon les législations nationales et peuvent être de fond ou de forme. Les critères de fond concernent par exemple la restriction qui veut que l'on ne recueille d'informations en matière criminelle que dans les cas de crimes organisés ou de crimes représentant une menace pour la société. Un critère de forme est par exemple le fait qu'un ministère de la Justice, un ministère des Affaires intérieures, un juge ou un procureur donnent mandat pour collecter, pendant une période limitée et, si possible, dans une zone géographique déterminée, des informations en matière criminelle sur un groupe bien défini de personnes soupçonnées d'être impliquées dans un secteur rigoureusement circonscrit de la criminalité. La question à laquelle il faut alors répondre est de savoir si ce mandat devrait être un document accessible au public, soit dès le départ, soit dès que sa divulgation ne risquerait plus de compromettre la bonne marche de l'enquête.

5.2.2 Stockage de données sur des personnes liées à des cibles d'informations en matière criminelle

Le principe consiste à traiter les données en matière criminelle concernant un groupe de personnes – que la loi doit définir avec précision –, à l'égard desquelles il n'y a pas encore de raisons concrètes de penser qu'elles ont commis un délit. L'établissement du profil de ces personnes, du point de vue de leurs comportements criminels, oblige à stocker des données concernant également des tierces personnes non soupçonnées, même si elles ne répondent pas aux critères des cibles d'informations en matière criminelle. On peut à cet égard distinguer deux types de tierce personne :

(1) la tierce personne avec laquelle les cibles des informations en matière criminelle sont en contact, soit physiquement (d'après les observations concrètes), soit par voie de télécommunications (d'après ce qu'a montré la surveillance électronique de ses moyens de communication, c'est-à-dire téléphone, fax, courrier électronique, etc.);

(2) la tierce personne qui informe la police (informateurs, qui sont souvent eux-mêmes des délinquants) : compte rendu de toutes les conversations de l'informateur avec la police, voire de son comportement, pour pouvoir déterminer sa fiabilité et maintenir une surveillance des policiers qui sont en contact avec lui.

Les données concernant les tierces personnes visées aux points (1) et (2) doivent être conservées séparément des données sur les "cibles" des informations en matière criminelle puisqu'elles sont collectées pour des finalités différentes. Les données en (1) doivent être limitées au strict nécessaire pour permettre d'avoir une idée claire du sujet. Le stockage n'autorise pas à établir le profil de ces contacts. Les données en (2) peuvent être plus étendues pour permettre de juger, en cas de contestation, la légalité de la collecte des données (et donc la recevabilité des moyens de preuve) auprès de ces informateurs. Il peut en résulter que les données réunies sur les personnes en (2) sont plus complètes que sur les personnes en (1) dans la mesure où la collecte des données répond dans les deux cas à des fonctions différentes.

Cette différence de fonction implique aussi que les décisions concernant les interrogatoires, les recoupements et les recherches devraient être justifiées en fonction des circonstances propres à chaque ensemble de données, compte tenu des raisons qui justifient leur traitement. L'utilisation de ces données doit être réglementée de manière plus stricte encore. L'objet des données visées au point (1) est d'apporter des informations sur une personne "cible" ; celui des données visées au point (2) est de déterminer la fiabilité de l'informateur. Le traitement par recoupement, combinaisons et recherches de données en (1) et (2) pour trouver des schémas de contacts entre des délinquants et établir de nouvelles cibles de renseignements criminels peut être considéré comme une forme d'utilisation compatible. Cela est moins évident lorsque les données sont utilisées pour répondre à un objectif qui se situe en dehors de la mission de la police. Au vu de l'article 9 de la Convention N° 108, un tel usage exigerait une base juridique explicite.

5.2.3 Pendant quelle durée peut-on stocker les informations en matière criminelle ?

La loi se doit d'être explicite sur la durée de stockage des informations en matière criminelle. On pourrait songer à un délai de quelques années à compter du jour où la dernière donnée pertinente à été ajoutée au fichier. A l'issue de cette période, on pourrait envisager un examen périodique (comme celui prévu à l'article 112 de l'Accord de Schengen). Si cet examen conclut qu'il n'existe pas de motifs suffisants pour justifier la conservation de ces données, celles-ci devraient en principe être détruites. La protection des données ne justifie pas de stocker des informations pour la simple raison "qu'elles pourraient éventuellement servir dans un avenir non prévisible". Cette formule n'exclut pas la possibilité de décider, à l'issue des examens successifs, de conserver les données, le cas échéant pour une durée indéterminée. Cette possibilité doit être acceptée chaque fois qu'il existe de bonnes raisons de le faire. On peut également penser à un système plus strict de suppression obligatoire après un certain laps de temps.

5.2.4 Remarques finales sur les informations en matière criminelle

Réglementer les informations en matière criminelle n'a de sens que si le stockage et l'utilisation de données en matière criminelle sur d'autres personnes non suspectées ne sont autorisés qu'à des fins spécifiques et pour de courtes périodes définies par la loi.

Proposition: Il est recommandé que les Etats membres définissent de manière restrictive, dans leur législation nationale, les "cibles" qui peuvent faire l'objet d'informations en matière criminelle. La loi devrait définir clairement un délai pour l'examen périodique de l'opportunité de prolonger le stockage.

La Commission nationale fait sienne les principales observations et réserves majeures exprimées dans ces documents.

V) L'insertion d'un droit d'accès indirect

La Commission nationale considère que tant au niveau de l'article 17-1 nouveau que de l'article 17-2 nouveau, il convient d'introduire un droit d'accès qui, pour des raisons évidentes, ne saurait être qu'indirect, comme celui d'ores et déjà prévu à l'article 17 de la loi du 2 août 2002.

VI) Sanctions pénales

A) Par analogie avec l'article 17 paragraphe 3 de la loi du 2 août 2002, il conviendrait de prévoir également des sanctions pénales aux articles 17-1 et 17-2 nouveaux.

B) En vue d'éviter des redites superflues dans la loi, et pour marquer la cohérence et simplifier la lecture du texte, la Commission nationale suggère dans ce contexte comme alternative de prévoir que la surveillance des nouvelles dispositions légales des articles 17-1 et 17-2 soit assurée par l'autorité de contrôle instaurée à l'article 17, paragraphe 2 actuel de la loi et de réserver un nouvel article 17-3 relatif aux sanctions pénales uniformes, applicables tant à l'article 17 actuel de la loi qu'aux articles 17-1 et 17-2 nouveaux, dont la teneur pourrait être celle de l'actuel paragraphe 3 de l'article 17.

VII) La fin du régime général de l'autorisation par voie réglementaire ?

A) De façon plus générale, la Commission nationale s'interroge quant à la portée de l'article 17-2 nouveau (qui apparaît plus étendue que l'intitulé même de l'avant-projet de loi sous avis) et sur le rôle résiduel que jouera à l'avenir l'actuel article 17 paragraphe 1er lettre (a), voire même lettres (a), (b) et (c).

En effet, à la lecture de l'avant-projet de loi sous avis, l'on peut se demander si les dispositions exorbitantes de l'article 17-2 nouveau ne conduiront pas à saper la vocation du régime général de l'autorisation par voie réglementaire visée à la lettre (a) de l'article 17 paragraphe 1er aux termes duquel font l'objet d'un règlement grand-ducal les traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions pénales qui sont réservés, conformément à leurs missions légales et réglementaires respectives, aux organes du corps de la police grand-ducale, de l'Inspection générale de la police et de l'administration des douanes et accises.

Aux yeux de la Commission nationale, la même question peut être posée, a fortiori, pour les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique, et les traitements de données dans des domaines du droit pénal effectués en vertu de conventions internationales, d'accords intergouvernementaux ou dans le cadre de la coopération avec l'Organisation internationale de police criminelle (OIPC – Interpol), traitements qui sont visés aux lettres b) et c) de l'article 17 paragraphe 1er de la loi. Mais cela impliquerait, en parallèle, la nécessité d'adapter en ce sens la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat.

Ainsi décidé à Luxembourg en date du 4 mai 2005

La Commission nationale pour la protection des données

(*s.*) Gérard Lommel	(*s.*) Pierre Weimerskirch	(*s.*) Thierry Lallemang
Président	Membre effectif	Membre effectif

Délibération n°73/2005 du 1er juillet 2005 de la Commission nationale pour la protection des données relative à la demande d'autorisation préalable en matière de surveillance du courrier électronique, de l'Internet et du réseau informatique de la société anonyme ODYSSEY ASSET MANAGEMENT SYSTEMS S.A. Luxembourg

I. Objet de la demande

Vu la demande d'autorisation introduite par la société anonyme ODYSSEY ASSET MANAGEMENT SYSTEMS S.A., établie et ayant son siège social à L-2540 LUXEMBOURG, Espace Kirchberg-Eolis, 26-28, rue Edward Steichen, (ci-après désignée « la requérante »), par courrier du 7 octobre 2003, sur base de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après en abrégé « la loi »),

Vu les compléments d'informations fournis par la requérante par courrier du 16 mars 2004,

La Commission nationale pour la protection des données (ci-après « Commission nationale ») constate que le traitement de données à caractère personnel envisagé qui fait l'objet de la demande d'autorisation consiste dans des mesures de surveillance du courrier électronique, de l'Internet et du réseau informatique.

II. Quant à la compétence

La Commission nationale se déclare compétente pour examiner la demande d'autorisation lui présentée sur base des articles 10, 11, 14 et 32 paragraphe 3 lettre d) de la loi.

III. Quant à la recevabilité

La Commission nationale déclare la demande d'autorisation recevable, étant donné qu'elle comprend toutes les informations obligatoires mentionnées à l'article 14, paragraphe 2 de la loi.

IV. Généralités

A) L'application de la loi du 11 août 1982 concernant la protection de la vie privée et de la loi du 30 mai 2005 relative aux dispositions spécifiques de protection dans le secteur des communications électroniques :

L'enregistrement des données de communications électroniques tombe dans le champ d'application de diverses autres dispositions légales qu'il convient de rappeler brièvement avant de statuer sur le fond de la demande telle que présentée par la requérante :

1) La Constitution

L'article 28 de la Constitution instaure le secret des correspondances privées en disposant que :

« Le secret des lettres est inviolable. - La loi détermine quels sont les agents responsables de la violation du secret des lettres confiées à la poste. La loi réglera la garantie à donner au secret des télégrammes. »

2) La Convention européenne des Droits de l'Homme

La Convention européenne des Droits de l'Homme dispose en son article 8 alinéa 1er que « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ».

3) La Charte des droits fondamentaux de l'Union européenne

La Charte des droits fondamentaux de l'Union européenne (adoptée lors du Conseil européen de Nice, le 7 décembre 2001, et proclamée par les présidents du Conseil, du Parlement européen et de la Commission) prévoit en son article 7 que „Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications".

Force est de constater que ni la Convention européenne des Droits de l'Homme ni la Charte des droits fondamentaux de l'Union européenne ne font de distinction entre correspondances postales et électroniques.

4) Le Code pénal

L'article 460 du code pénal prévoit que :

« Quiconque sera convaincu d'avoir supprimé une lettre confiée à la poste, ou de l'avoir ouverte pour en violer le secret, sera puni d'un emprisonnement de huit jours à un mois et d'une amende de 251 euros à 2.000 euros, ou d'une de ces peines seulement. »

Cette inviolabilité des correspondances est encore renforcée pour certaines personnes au regard de l'article 149 du code pénal aux termes duquel :

« Sera puni d'un emprisonnement de quinze jours à deux mois et d'une amende de 251 euros à 5.000 euros, tout fonctionnaire ou agent du Gouvernement, tout employé du service des postes et des télégraphes, qui aura ouvert ou supprimé des lettres confiées à la poste, des dépêches télégraphiques, ou qui en aura facilité l'ouverture ou la suppression. »

5) La loi du 11 août 1982 concernant la protection de la vie privée :

« Art. 2. Est puni d´un emprisonnement de huit jours à un an et d´une amende de deux mille cinq cent un à cinquante mille francs, ou d´une de ces peines seulement, quiconque a volontairement porté atteinte à l´intimité de la vie privée d´autrui… .

3° en ouvrant sans l'accord de la personne à laquelle il est adressé ou de celle dont il émane, un message expédié ou transmis sous pli fermé, ou, en prenant connaissance, par un appareil quelconque, du contenu d'un tel message ou en supprimant un tel message. …

Art. 3. Est puni des peines prévues à l´article 2, celui qui a sciemment placé ou fait placer un appareil quelconque dans le but de commettre l´une des infractions prévues par l´article 2 ou d´en rendre possible la perpétration.

Art. 4. Est puni des peines prévues à l´article 2 celui qui, sans le consentement des personnes visées à cet article, a sciemment conservé, porté ou laissé porter à la connaissance du public ou d´un tiers, ou utilisé publiquement ou non, tout enregistrement ou document obtenu à l´aide d´un des faits prévus à cet article… ».

Il ressort des travaux parlementaires relatifs à la loi de 1982 que cette disposition élargit le champ d'application de l'inviolabilité des correspondances :

« Enfin, .l'article 2 punit celui qui, sans l'accord de la personne à laquelle il est adressé ou de celle dont il émane, a ouvert un message expédié ou transmis sous pli fermé, ou, par un procédé technique quelconque, a pris connaissance du contenu d'un tel message ou a supprimé un tel message. Le texte reprend en substance les articles 149 et 460 du Code pénal tout en élargissant leur champ d'application. Le secret d'une lettre est protégé non seulement aussi longtemps que cette missive reste confiée à la poste, mais également à d'autres stades, par exemple lorsqu'elle se trouve dans la boîte aux lettres du destinataire. En outre, pour être protégé par la loi, le message ne doit pas nécessairement avoir été transmis par la poste. Est également puni celui qui sans avoir ouvert la lettre a cependant pris connaissance de son contenu par un moyen technique. » (cf. document parlementaire 2177/00, p.1683).

6) La directive 2002/58/CE (directive « vie privée et communications électroniques »)

L'article 1, paragraphe 2, de la Directive 2002/58/CE prévoit que :

« Champ d'application et objectif

2. Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1… ».

Le Considérant 10 de la Directive 2002/58/CE énonce à ce sujet que : « Dans le secteur des communications électroniques, la directive 95/46/CE est applicable notamment à tous les aspects de la protection des droits et libertés fondamentaux qui n'entrent pas expressément dans le cadre de la présente directive, y compris les obligations auxquelles est soumis le responsable du traitement des données à caractère personnel et les droits individuels. La directive 95/46/CE s'applique aux services de communications électroniques non publics...».

Le Considérant 23 de la Directive 2002/58/CE énonce que : « (23) La confidentialité des communications devrait également être assurée dans les transactions commerciales licites. Au besoin et sous réserve d'une autorisation légale, les communications peuvent être enregistrées pour servir de preuve d'une transaction commerciale...».

L'article 5 de la Directive 2002/58/CE prévoit que :

« Confidentialité des communications

1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité.

2. Le paragraphe 1 n'affecte pas l'enregistrement légalement autorisé de communications et des données relatives au trafic y afférentes, lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale ».

La directive prévoit donc la possibilité, pour les Etats membres, de permettre ce type d'enregistrement à des fins de preuve de transactions ou de toutes autres communications commerciales.

Cependant, l'exception vise seulement les transactions commerciales opérées dans le cadre des usages professionnels licites.

Dans la mesure où cette exception vient restreindre un droit fondamental, elle doit faire l'objet d'une explicitation au niveau du droit national avant de pouvoir être invoquée.

Cette directive a été transposée en droit interne par la loi du 30 mai 2005 relative aux dispositions spécifiques de protection dans le secteur des communications électroniques, dont l'entrée en vigueur est prévue pour le 1er juillet 2005, (Mém. A. n° 73 du 7 juin 2005, p. 1168).

7) La loi du 30 mai 2005 relative aux dispositions spécifiques de protection dans le secteur des communications électroniques

Cette loi du 30 mai 2005 transpose la directive 2002/58/CE du 12 juillet 2002 dite directive « *vie privée et communications électroniques* ». Il s'agit d'une réglementation sectorielle puisque la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel s'applique à tout ce qui n'est pas spécialement prévu par la prédite loi.

Quant à la lettre d) de l'article 4, paragraphe 3, de la loi précitée du 30 mai 2005, elle n'englobe pas le bout de phrase de l'article 5 paragraphe 2 de la directive 2002/58/CE « ou de toute autre communication commerciale », alors qu'elle est libellée comme suit :

« qu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ».

« Si le présent amendement n'était pas apporté à l'article 4, il serait possible que la confidentialité de la communication ne soit pas assurée entre l'abonné et l'utilisateur dans la mesure où il s'agirait de personnes différentes. Ainsi, si l'abonné est une entreprise et l'utilisateur est son salarié, cela laisserait entrevoir la licéité d'une mesure de surveillance opérée par l'entreprise abonnée sur son salarié utilisateur, pourtant contraire notamment à la confidentialité prescrite par l'article 5 de la Directive, et qui serait par ailleurs contraire tant à la loi du 11 août 1982 concernant la protection de la vie privée, qu'au régime d'autorisation institué par les articles10, 11 et 14 de la loi du 2 août 2002 précitée » (document parlementaire n° 5181/06, p. 2 et 3).

« Par amendement du 22 juillet 2004, le gouvernement a proposé de reformuler le paragraphe (2) en supprimant la référence à l'abonné et à l'utilisateur final. En effet, la confidentialité doit être telle qu'elle vaut à l'égard de toute personne autre que l'utilisateur. Or, l'abonné n'est pas nécessairement l'utilisateur et la confidentialité devrait donc également jouer à son égard. Sans cet amendement, il aurait été possible que la confidentialité de la communication ne soit pas assurée entre l'abonné et l'utilisateur (par exemple: si l'abonné est une entreprise et l'utilisateur est son salarié, on aurait pu arguer qu'une mesure de surveillance opérée par l'entreprise abonnée sur son salarié utilisateur soit possible, ce qui aurait permis de contourner la loi du 11 août 1982 concernant la protection de la vie privée et la loi du 2 août 2002). Le Conseil d'Etat s'est déclaré d'accord avec cet amendement. La Commission a fait de même. » (document parlementaire n° 5181/14, p. 7).

« 3. la question de l'autorisation légale : dans son avis du 29 janvier 2004, la Chambre de Commerce souligne que la législation luxembourgeoise ne prévoit pas d'autorisation légale pour l'enregistrement des communications électroniques à des fins de preuve commerciale tel que l'exige l'article 5, paragraphe (2) de la directive. Elle estime qu'il est dès lors souhaitable que le projet de loi 5181 contienne une disposition autorisant les enregistrements à des fins de preuve commerciale. Le paragraphe 3 (d) a fait l'objet d'un amendement gouvernemental : les termes „légalement autorisé" ont été supprimés, puisque c'est précisément en vertu de la présente disposition que l'enregistrement est légalement autorisé. La suppression de ces termes évite ainsi la confusion qui pourrait naître quant à l'éventuelle nécessité d'une autorisation légale spéciale, en plus de celle résultant de la disposition elle-même » (document parlementaire n° 5181/14, p. 8).

Il ressort dès lors clairement des travaux préparatoires à la loi du 30 mai 2005 que celle-ci ne déroge ni à la loi-cadre du 2 août 2002, en particulier au régime d'autorisation instaurée par les articles 10, 11 et 14, ni à la loi du 11 août 1982 concernant la protection de la vie privée.

En revanche, le responsable du traitement n'est plus tenu d'obtenir le consentement des parties à la communication pour en effectuer l'enregistrement, à condition « qu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale », conformément à l'article 4, paragraphe 3, lettre d) de la loi précitée du 30 mai 2005.

Ainsi, tout enregistrement de communications, tel qu'effectué par la requérante, continue à être soumis à l'obtention préalable du consentement de toutes les parties à la communication, en application de l'article 2 de la loi précitée du 11 août 1982, à moins qu'il ne s'agisse d'un enregistrement de communications effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale, autorisé de par la loi du 30 mai 2005.

8) La Doctrine

A) La surveillance des courriers électroniques dans l'entreprise

(par Stéphan Le GOUEFF ; voir sous http://www.avocats.com/)

« Il faut relever que ces textes (relatifs au secret des correspondances) ne font aucune distinction selon que le courrier est transmis sur un lieu de travail ou au domicile d'un employé.

La protection semble devoir simplement être accordée à toute correspondance qui relève de la vie privée, c'est-à-dire selon la définition retenue par les parlementaires lors de l'adoption de cette loi "à tout ce qui doit être caché des autres".

Bien que les textes ne soient pas entièrement clairs, on peut présumer que la confidentialité ne devrait porter que sur les e-mails à caractère privé et non sur ceux adressés à l'entreprise dans la boîte de réception de l'un de ses employés. Dans la pratique, il risque toutefois d'être difficile de distinguer les uns des autres s'ils sont mélangés dans la boîte de réception de la messagerie électronique de l'employé. Dans ce cas, il serait difficile d'avoir accès aux messages de l'entreprise sans également violer la confidentialité des messages à caractère privé.

Les entreprises luxembourgeoises ne devraient donc pas, en principe, pouvoir procéder à un contrôle des courriers électroniques de leurs employés, sauf dans l'hypothèse prévue par la loi de 1982, où ces derniers auraient consenti préalablement à un tel contrôle.

Une solution pourrait consister pour ces employeurs à insérer dans les contrats de travail une clause suivant laquelle l'employé donnerait expressément son consentement à ce que son courrier électronique, reçu sur l'adresse électronique de l'entreprise (par opposition à une adresse de type "hotmail" personnelle de l'employé), sur l'ordinateur mis à sa disposition par l'entreprise, soit considéré comme étant le courrier de l'entreprise et puisse être accédé par l'entreprise ou puisse faire l'objet d'une surveillance de l'entreprise. Il pourrait également être convenu que la messagerie électronique ne peut-être utilisée qu'à des fins professionnelles et non pour des messages de nature privée. »

B) Cybersurveillance des salariés et règles de preuve devant les Prud'hommes

(par Geneviève Folzer et Mathieu Abboud, avocats au barreau de Luxembourg, inscrits au barreau de Strasbourg ;

http://www.strasbourg.cci.fr/point_economique/221/cybersurveillance_des_salaries.pdf)

« Il y a des e-mails personnels et d'autres professionnels. Tous sont soumis au secret des correspondances. Pour les distinguer, l'employeur peut demander que chaque e-mail personnel se signale comme tel dans son intitulé. Il peut également demander au salarié de créer un « folder » dédié aux correspondances personnelles. Ces solutions devraient offrir à l'employeur qui consulte des correspondances dites « professionnelles » la protection de l'excuse de bonne foi de l'article 226-15 du code pénal (notons que les autorités publiques conformément aux articles 226-13 et 432-9 du code pénal n'en bénéficient pas). »

C) Courrier électronique : les suites de la décision de la Cour de Cassation

(par Olivier Iteanu, avocat, voir sous http://www.journaldunet.com/juridique/juridique011009.shtml)

« L'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur (Affaire NIKON, Cass. soc. 2 octobre 2001).

Nous voyons plutôt par les juges la consécration d'un principe selon lequel il y a dans l'entreprise des correspondances privées qui appartiennent à l'entreprise et d'autres aux salariés et que ces dernières ne peuvent venir prouver une faute ayant motivé un licenciement. »

D) L'Internet et les relations de travail dans l'entreprise

(par Héloïse Deliquiet, Avocat, Fidal ; Géraldine Michel, Avocat, Fidal, Docteur en droit ; Maud Haranger et Jean-Baptiste Blanc, Juristes Fidal ; voir sous http://www.fidal.fr/Fichiers_articles/affichage.cfm?num=211).

« La question se pose, en pratique, de déterminer et d'identifier ce qu'il faut entendre d'un courrier électronique à caractère personnel et privé. Le rapport de la Commission nationale de l'informatique et des libertés (CNIL) pour 2001 énonce sur ce point qu'il « doit être généralement considéré qu'un message envoyé ou reçu depuis le poste du travail mis à disposition par l'entreprise ou l'administration revêt un caractère professionnel, sauf indication manifeste dans l'objet du message ou dans le nom du répertoire où il pourrait avoir été archivé par son destinataire qui lui conférerait alors le caractère et la nature d'une correspondance privée ».

Ainsi, si un message est adressé au salarié sans que ne figure la mention « personnel » dans son objet, il est présumé avoir un caractère professionnel.

Selon la jurisprudence rendue en matière de courrier postal, lorsqu'une correspondance est adressée à un membre d'une organisation avec son nom et son appartenance à cette organisation, sans indication du caractère personnel de la correspondance, et que cette correspondance a été adressée à l'individu en sa qualité de membre de l'organisation, cette dernière est le véritable destinataire du courrier : il n'y a pas d'atteinte au secret des correspondances si l'employeur fait ouvrir le courrier. Et l'on s'accorde à reconnaître à cette jurisprudence qu'elle est parfaitement transposable aux messages électroniques.

Concrètement, il est donc recommandé aux employeurs soit de faire mettre en place par leurs salariés une double boite de messagerie permettant de distinguer les messages personnels et les messages professionnels, soit d'inviter ces derniers à classer les messages reçus dans un dossier identifié comme « personnel » ou « privé » lorsqu'ils présentent un tel caractère. »

E) Les limites du pouvoir de cybersurveillance de l'employeur

(par Jérôme Gabourin, Vincent Jouvet, Anh Trinh, Sébastien Vergendo ; Relations individuelles & Collectives dans l'Entreprise ; PARIS XII. DESS RHSE – 2003 ; voir sous http://www.fjpansier.com/DESSCRETEIL/DESS%20RH%202002-2003/

CYBERSURVEILLANCE/final-rapport.doc)

« C'est, à notre avis, le véritable apport de l'arrêt sur le plan juridique : la Cour de cassation affirme que la règle du secret des correspondances s'applique aux messages électroniques dès lors qu'ils sont « personnels ». Les salariés pourraient donc disposer désormais d'un espace privatif sur leur disque dur, d'un vestiaire électronique (p. 22).

Si l'on admet, avec la Cour de cassation, que tous les messages « personnels » sont de manière générale des correspondances protégées par le secret, il convient alors de définir ce qu'est un e-mail personnel. Il sera donc possible, à notre avis, d'écarter devant les juges du fond, dans un certain nombre d'hypothèses, l'application de la règle énoncée par la Cour de cassation, notamment lorsque le message concerne l'activité professionnelle (exemples du fichier privé joint à un e-mail de nature professionnelle ou de l'e-mail « mixte » évoquant un dossier et les relations extraprofessionnelles entre deux collègues de travail) (p.23).

A l'instar de la CNIL, il est conseillé de raisonner par analogie à la jurisprudence relative à la correspondance papier. De fait, le caractère professionnel des mails devra être reconnu en l'absence des mentions « privé » ou « personnel » dans le titre de ce dernier. Il existe donc une présomption du caractère professionnel des e-mails. Par conséquent, l'employeur a intérêt à ne pas interdire, mais seulement recommander à ses salariés un usage modéré de leur messagerie électronique à des fins privées (p. 25).

La question se pose exactement comme en matière de courriers postaux. Si le caractère privé du message est apparent, l'employeur ne pourra pas en prendre connaissance. En revanche, si rien n'est précisé, le message est présumé professionnel. Le Tribunal de Grande Instance de PARIS a, dans son jugement du 02 novembre 2000 affirmé le principe selon lequel il convient d'assimiler le courrier électronique à une correspondance privée. Les prévenus ayant fait appel de ce jugement, il faut cependant attendre l'arrêt de la Cour d'Appel pour pouvoir éventuellement confirmer ce point. Si l'on s'en tient à ce jugement, le courrier électronique professionnel ou privé sera toujours considéré comme de la correspondance privée » (p. 26).

F) La surveillance de l'employé de banque : la vie privée et la protection des données

« Le droit de surveillance de l'employeur est limité. L'employeur ne peut pas violer le secret des correspondances. Il ne peut donc pas produire en justice, en tant que preuve, le contenu des messages e-mail ou des télécopies ou encore le contenu de l'enregistrement d'une conversation téléphonique, ce qui revient à affirmer le principe d'une vie privée sur le lieu de travail ». (Sophie WAGNER-CHARTIER et Héloïse BOCK, Droit bancaire et financier au Luxembourg, volume 1, p. 421).

G) Internet et libertés : quelques repères

« En toute hypothèse, les deux arrêts rendus par la cour d'appel de Montpellier le 6 juin 2001 et par la Chambre sociale de la Cour de cassation le 2 octobre 2001 ont en commun d'admettre le contrôle par l'employeur de l'usage fait de la messagerie par le salarié - contrairement à ce qui a été souvent écrit au sujet du second de ces arrêts - dès lors évidemment que ce contrôle respecte les dispositions légales. Et c'est sur ce terrain de la légalité du contrôle que les deux juridictions se situent pour considérer, en présence d'un contrôle jugé illégal, que la preuve est illicite. Dans la seconde espèce, il est permis de considérer que la Cour de cassation aurait donné une autre solution au litige si la preuve de la faute grave retenue par la cour d'appel pour motiver le licenciement (une activité parallèle entretenue pendant les heures de travail) avait été apportée non par la production du contenu de messages émis et reçus par le salarié, que l'employeur avait découverts dans un fichier intitulé "personnel" de l'ordinateur de ce dernier, mais par la preuve de l'utilisation du courrier électronique aux mêmes fins, preuve faite grâce à un processus d'identification des messages, sans lecture de ceux-ci. Infiniment plus difficile et plus coûteuse, cette preuve, de l'avis de certains techniciens, n'est pas pour autant impossible à apporter.

Statuant sur l'appel formé à l'encontre du jugement du tribunal correctionnel de Paris du 2 novembre 2000 précité, la cour d'appel de Paris, dans un arrêt du 17 décembre 2001, a considéré que "la préoccupation de la sécurité du réseau justifiait que les administrateurs de systèmes et de réseaux fassent usage de leurs positions et des possibilités techniques dont ils disposaient pour mener les investigations et prendre les mesures que cette sécurité imposait - de la même façon que la Poste doit réagir à un colis ou une lettre suspecte. - Par contre la divulgation du contenu des messages (...) ne relevait pas de ces objectifs". Réformant la motivation du jugement, elle a confirmé ce dernier sur la culpabilité, sur le fondement de l'article 432-9, alinéa 2, du Code pénal. »

(cf. Emmanuel TOIS, rapport annuel 2001 de la Cour de Cassation française ; http://www.courdecassation.fr/_rapport/rapport.htm).

H) Messagerie électronique de l'entreprise : le pouvoir de contrôle de l'employeur à l'épreuve du secret des correspondances

« On n'en aurait pas terminé sur ce terrain si n'était pas évoquée l'incertitude quant au champ d'application du secret des correspondances. Ce secret s'applique-t-il aux informations relatives ou nécessaires à l'acheminement des correspondances électroniques tels que l'objet de la correspondance ou le destinataire de celle-ci ? Ces éléments peuvent permettre de caractériser des actes de concurrence déloyale notamment si l'un des destinataires du salarié est un concurrent de l'entreprise sans même ouvrir le contenu du message. La jurisprudence devra se prononcer sur ce point.

Outre ces incertitudes, restent encore les interrogations quant à la possibilité pour l'employeur d'utiliser certains outils techniques de protection du réseau tels que les pare-feu. Permettant de supprimer un message comportant un virus ou émanant d'une origine prohibée, ce mécanisme ne tombe-t-il pas sous le coup du secret des correspondances ? Nous ne le pensons pas dès lors que les salariés et le comité d'entreprise auront été informés de la mise en place d'un tel dispositif nécessaire à la

sécurité du réseau mais la jurisprudence ne s'est pas encore prononcée sur ce point. » (cf. Florence BITAN, dans Communication – Commerce électronique, JCL, Juin 2004, p. 12).

9) La jurisprudence

Lorsqu'une correspondance est adressée à un membre d'une organisation avec son nom et son appartenance à cette organisation, sans indication du caractère personnel de la correspondance, et que cette correspondance a été adressée à l'individu en sa qualité de membre de l'organisation, cette dernière est le véritable destinataire du courrier, de sorte qu'il n'y a pas d'atteinte au secret des correspondances si l'employeur fait ouvrir le courrier (cf. Cour de Cassation fr., chbre crim., 16 janvier 1992, Gaz. Pal., 1992, somm., p. 296).

« Le secret des correspondances visé par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales doit s'appliquer également aux technologies nouvelles de transmission de la correspondance, peu importe l'endroit à partir duquel ces courriers électroniques sont envoyés ou réceptionnés. Dans cette optique, l'admission du droit de regard de l'employeur sur le contenu des messages e-mail envoyés par ses salariés, sur son matériel, au lieu de travail, doit se cantonner à l'établissement de la preuve d'un comportement fautif ou déloyal, c'est-à-dire que l'employeur peut prouver une utilisation à des fins privées pendant les heures de travail par un salarié de l'ordinateur mis à sa disposition par l'entreprise, à partir d'indicateurs généraux, inhérents à l'ordinateur, et établir ainsi la date, la fréquence et le volume d'une telle utilisation, sans pouvoir prendre une connaissance concrète et exacte du contenu des courriers électroniques protégés par le secret de la correspondance… . L'employeur peut cependant prendre connaissance, dans le cadre de ses pouvoirs de chef d'entreprise, du contenu d'autres fichiers établis par le salarié et non protégés par le secret de la correspondance. Il peut de même établir une utilisation pour le propre compte du salarié du fax de l'entreprise, sans qu'il soit autorisé à produire le corps des courriers envoyés. » (cf. Trib. Trav, Luxembourg, 20 novembre 2001, Laurent c. Dyckerhoff Matériaux Achat S.A., cité par G. CASTAGNERO) (Droit du travail luxembourgeois, p.71).

B) La notion de surveillance

Par ailleurs, se pose la question si l'enregistrement des communications électroniques constitue une surveillance au sens de la loi du 2 août 2002.

L'article 2, lettre (q), de la loi définit la "surveillance" comme étant « toute activité faisant appel à des moyens techniques en vue de détecter, d'observer, de copier ou d'enregistrer les mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile ».

Cette définition est suffisamment large pour appréhender l'ensemble des techniques de surveillance y compris la vidéosurveillance, la surveillance électronique et informatique (cf. document parlementaire 4735/00, p. 27).

Ainsi la loi luxembourgeoise a entendu soumettre à un examen préalable par l'autorité de contrôle ce type de traitement de données à caractère personnel à la lumière du considérant 53 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, aux termes duquel :

« …certains traitements sont susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées, du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, ou du fait de l'usage particulier d'une technologie nouvelle; qu'il appartient aux Etats membres, s'ils le souhaitent, de préciser dans leur législation de tels risques ».

Il s'ensuit que tout traitement de données à caractère personnel requiert une autorisation préalable de la part de la Commission nationale au titre de l'article 11 de la loi pour le cas où ces données sont effectivement exploitées dans un but de surveillance, c'est-à-dire servent « à des fins » de surveillance.

Tel est le cas de l'hypothèse envisagée consistant dans l'enregistrement des communications électroniques des salariés.

C) Les traitements à des fins de surveillance

« Il se peut qu'un même traitement tombe dans le champ d'application soit de l'article 10 soit de l'article 11 en fonction de la personne concernée. Par exemple, une caméra dans une grande surface tombe sous le coup de l'article 10 si la personne concernée est un client, même potentiel, du magasin et sous celui de l'article 11 si la personne concernée est un salarié employé par le propriétaire de ce magasin. » (cf. document parlementaire 4735/13, p. 17).

En l'espèce, les personnes concernées par l'enregistrement des communications électroniques sont tant « tous les collaborateurs (employés) » que « les consultants externes effectuant une prestation pour le compte d'Odyssey et ayant accès au réseau interne d'Odyssey ».

Quel que soit le régime applicable, la ratio legis exige que les moyens de surveillance ne soient pas cachés (principe de la transparence) (cf. document parlementaire 4735/13, p. 17).

En effet, suivant l'article 4, paragraphe 1er de la loi, « le responsable du traitement doit s'assurer que les données qu'il traite le sont loyalement et licitement, et notamment que ces données sont :

(a) collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ;

(b) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ;

(c) exactes et, si nécessaire, mises à jour; toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;

(d) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées… ».

La Commission nationale rappelle qu'un traitement à des fins de surveillance (que ce soit le régime général visé à l'article 10 ou le régime particulier prévu à l'article 11) doit, pour être licite, être effectué conformément aux dispositions de l'article 4 de la loi (cf. document parlementaire 4735/13, p. 17).

Dérogeant à l'article 5 traitant des conditions de légitimité générales, l'article 10 de la loi détermine les hypothèses dans lesquelles une surveillance peut être effectuée qui sont au nombre de trois (cf. document parlementaire 4735/13, p. 17). Les cas d'ouverture permettant cette surveillance sur le lieu de travail sont énumérés à l'article 11 paragraphe 1er de la loi, cette énumération étant à considérer elle aussi comme limitative (cf. document parlementaire 4735/00, p. 98). En effet, l'exposé des motifs du projet de loi figurant dans le document parlementaire 4735/00 (p. 99) évoque le « caractère limitatif des cas légitimant la surveillance sur le lieu de travail ».

Par ailleurs, les finalités éligibles étant limitativement énumérées, l'employeur ne saurait détourner les données recueillies pour une autre finalité incompatible avec celle qu'il entendait poursuivre initialement et qu'il a communiquée aux parties concernées en application de l'article 11, paragraphe (2) (cf. document parlementaire 4735/13, p. 21).

Il est utile de rappeler le contexte dans lequel l'article 11 a été élaboré, puisque la commission du travail et de l'emploi de la Chambre des Députés était convaincue de la nécessité de légiférer en la matière „avec la finalité d'instituer une protection efficace du salarié lui conférant toutes les garanties nécessaires pour faire respecter ses droits dans ce domaine". La commission des média et des communications partageait cette approche en y ajoutant qu'il convient de préciser les droits et obligations tant des salariés que des employeurs. L'article 11 intervient afin d'éviter des abus et un certain flou juridique préjudiciable pour tous (cf. document parlementaire 4735/13, p. 19).

Toujours selon la commission du travail et de l'emploi, l'intervention législative s'imposait alors qu'actuellement au Luxembourg « aucun texte légal ne fixe clairement les limites dans lesquelles un employeur peut surveiller ses salariés sur le lieu de travail ». La loi du 11 août 1982 concernant la protection de la vie privée peut trouver application dans certaines hypothèses, mais il faut être conscient du fait qu'elle ne vise en aucun cas directement et de façon générale la protection des droits des salariés. Il s'agit dès lors de voir de quelle façon le texte de l'article 11 pourra être amendé pour « répondre efficacement à sa finalité de protection des salariés », notamment en rencontrant les appréhensions exprimées dans les avis précités. Il faudra s'assurer que l'intervention législative comporte effectivement une amélioration par rapport à la situation juridique actuelle. Dans cette optique, le texte légal devra écarter tout moyen de trouver, par la voie de subterfuges plus ou moins ingénieux, de nouvelles possibilités d'abus au détriment des salariés (cf. document parlementaire 4735/07, p. 3).

En tout état de cause, la surveillance doit être adaptée au but légitime poursuivi et l'employeur doit recourir aux moyens de surveillance les plus protecteurs de la sphère privée du salarié (cf. document parlementaire 4735/13, p. 22).

Il appert des développements qui précèdent que le législateur luxembourgeois a institué pour les traitements à des fins de surveillance sur le lieu de travail un régime particulier qui déroge aux conditions de légitimité générales édictées à l'article 5 de la loi dans la mesure où l'article 11 trace un cadre de légalité plus strict pour ce genre de traitements.

V. Quant au fond :

A) Responsable du traitement et/ou sous-traitant :

La requérante s'est désignée elle-même comme responsable du traitement.

B) Légitimité :

La légitimité du traitement envisagé est motivée de la manière suivante :

« La société Odyssey travaille essentiellement pour le monde bancaire. Nous fournissons des logiciels qui traitent des données touchant leurs clients. Au sein de notre Société, des informations confidentielles appartenant aux banques peuvent aussi être enregistrées. Dans ces conditions, certaines de ces banques ont exigé que notre Société s'engage à renforcer nos mesures de sécurités (norme ISO 17 799) et à garantir la protection de leurs données. Dans certains cas, ces banques considèrent cette exigence de sécurité accrue comme une condition préalable à l'entrée en relations contractuelles avec Odyssey.

Sur base de ce qui précède et du paragraphe relatif aux « Finalités du Traitement » ci-dessous, il apparaît donc qu'Odyssey se situe bien dans les conditions d'application de l'article 11 (1) de la Loi en ce que le « traitement des données à des fins de surveillance sur le lieu de travail sera mis en œuvre pour les besoins de protection des biens de l'entreprise ».

> De plus, par le biais de notre règlement intérieur, nous nous sommes engagés auprès de nos collaborateurs à préserver leur sphère privée, en particulier le secret des correspondances. A cet égard, nous avons donc souligné que :
>
> Toutes les données circulantes ou stockées sur le réseau IT de la Société ou sur tout autre support (supports magnétiques, documentation papier) sont considérées de nature professionnelle. Il y a exception du moment qu'il est spécifiquement indiqué que la donnée est privée. Nos collaborateurs ont à disposition une place disque personnelle sur un serveur dédié à cet effet. De plus, il est conseillé pour l'usage des e-mails d'utiliser l'option « privé » ou de signaler dans le corps du message.
>
> La Société met à disposition des équipements (PC, e-mails, Internet…) à des fins professionnelles. Une utilisation privée est tolérée à condition qu'il n'y ait pas d'abus des ressources de l'entreprise.

La Société demande que tous les collaborateurs s'engagent à respecter les lois en vigueur (droit d'auteur, harcèlement sexuel, racisme…), les principes de confidentialité et de secret professionnel ainsi qu'à ne pas abuser des ressources de l'entreprise. »

En l'espèce, les personnes concernées par l'enregistrement des communications électroniques sont tant « tous les collaborateurs (employés) » que « les consultants externes effectuant une prestation pour le compte d'Odyssey et ayant accès au réseau interne d'Odyssey ».

Dans ces conditions, il y a donc lieu d'examiner la légitimité tant au regard de l'article 10 (« la personne concernée a donné son consentement ») qu'au regard de l'article 11 (« pour les besoins de protection des lieux de l'entreprise ») de la loi.

1) Au regard de l'article 10 : (tiers ayant accès aux équipements informatiques et au réseau interne d'Odyssey)

Force est de constater que la requérante n'a pas expressément fondé sa demande sur un des critères de légitimation tirés de l'article 10 de la loi.

Il s'agit dès lors de pallier à cette lacune par substitution afin d'accorder l'autorisation sollicitée d'une surveillance électronique visant les consultants externes amenés à prester leurs services en ayant recours aux outils informatique et au réseau interne d'Odyssey soumis à surveillance.

Les cas d'ouverture visés sous les lettres b) et c) de l'article 10 paragraphe 1er de la loi concernent à l'évidence d'autres types de surveillance que le contrôle de l'usage des outils informatiques et des communications électroniques.

L'article 10, paragraphe (1) de la loi prévoit que le traitement à des fins de surveillance ne peut être effectué que :

« (a) si la personne concernée a donné son consentement ».

Ce consentement doit être obtenu de façon individuelle, et il doit être libre, explicite et informé (cf. Enregistrement des télécommunications effectuées dans le cadre des services bancaires, Commission pour la protection de la vie privée, Belgique, N° JZ028M5_1, N° de rôle 01/2002 du 2002-08-22).

En ce qui concerne les clients, le consentement peut être obtenu par la signature des conditions d'utilisation du service proposé, à condition que l'attention du client soit attirée de façon suffisamment claire sur les conditions d'enregistrement des communications (cf. article 26 de la loi).

Une mention dans les conditions générales ne peut cependant être considérée comme suffisante. Les mentions doivent au moins figurer dans les conditions spécifiques liées à l'utilisation du service proposé, et l'attention de la personne concernée doit être attirée sur ces mentions, lorsqu'elle adhère au service.

Par analogie on pourrait étendre cette solution également aux contrats de louage d'ouvrage passés avec des consultants et sous-traitants.

La Commission nationale estime qu'il ne suffit pas que cette clause figure dans les conditions contractuelles aux quelles a adhéré l'entreprise qui met a disposition des consultants et collaborateurs externes mais que - s'agissant de libertés et droits fondamentaux des personnes physiques concernées -, celles-ci doivent avoir individuellement accepté la clause prévoyant la surveillance électronique durant leur activité pour être réputé y avoir marqué leur consentement.

2) Au regard de l'article 11 : (salariés)

D'emblée, il convient de rappeler qu'aux termes de l'article 11, paragraphe (1), dernier alinéa : « Le consentement de la personne concernée ne rend pas légitime le traitement mis en œuvre par l'employeur ».

En raison du lien de subordination entre l'employeur et le salarié - personne concernée, l'article 11 précise que le consentement de ce dernier ne rend pas légitime le traitement mis en oeuvre par l'employeur (cf. document parlementaire 4735/13, p. 21).

En revanche, la requérante devra pouvoir se prévaloir d'une condition de légitimité prévue à l'article 11 paragraphe 1er de la loi du 2 août 2002.

La teneur de la demande d'autorisation présentée amène la Commission nationale à considérer que la requérante entend invoquer vis-à-vis de ses salariés comme cas d'ouverture légitimant la surveillance sur le lieu de travail la lettre b) de l'article 11, paragraphe 1er indiquant comme finalité « (b) pour les besoins de protection des biens de l'entreprise ».

Il en suit que la demande d'autorisation de l'employeur doit être analysée par la Commission nationale à la lumière des dispositions expresses de l'article 11 de la loi ainsi que de la « ratio legis » ayant conduit à son adoption.

La notion de « protection des biens »

« Par les termes « les besoins de protection des biens de l'entreprise » le législateur a entendu viser en première ligne la prévention du vol et du vandalisme au moyen de caméras installées aux entrées et sorties de l'établissement, y compris les entrées du personnel. Relèvent également de la protection des biens de l'entreprise les moyens de surveillance destinés à s'assurer que des virus ne pénètrent pas le réseau d'ordinateurs, que des fichiers professionnels ne soient pas détruits, que le réseau ne soit pas encombré. On peut encore y ajouter les écoutes téléphoniques effectuées par des établissements de crédit et autres professionnels du secteur financier aux fins d'enregistrer les ordres des clients passés par téléphone à condition toutefois que tant le client ait donné son accord à un tel enregistrement et que le salarié ait été informé que les conversations téléphoniques passées par ce téléphone seront enregistrées » (cf. document parlementaire 4735/13, p. 21).

Il en résulte donc que de prime abord le critère de légitimation invoqué par la requérante peut être admis, encore faut-il cerner de plus près ce que le législateur vise par les termes « les besoins de protection des biens de l'entreprise ».

Pour ce faire, il y a également lieu de reproduire les finalités invoquées par la requérante pour la surveillance projetée :

« Toujours dans son règlement interne, Odyssey a précisé que la Société se réservait le droit d'entreprendre des contrôles uniquement pour les raisons suivantes :

- *La prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui (ex. : actes de piratage informatique, fuite de données relatives à la gestion du personnel ou de fichiers médicaux confidentiels, consultation de sites à caractère pornographique, pédophile, ou invitant à la discrimination raciale, ethnique, religieuse, etc.) ;*
- *La protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires (ex. : concurrence déloyale, divulgation de fichiers, violation des secrets d'affaire ou des droits de propriété intellectuelle de tiers, atteintes à l'image de marque de l'entreprise, etc.) ;*
- *La sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, y compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise (ex. : phénomènes d'engorgement, propagation de virus, etc.) ;*
- *Le respect de bonne foi des principes et règles d'utilisation des technologies en réseau de l'entreprise, notamment en vertu du règlement interne (ex. : abus des ressources de l'entreprise) ».*

La Commission nationale considère qu'il ressort des travaux parlementaires précités que le législateur n'a entendu autoriser les traitements à des fins de surveillance sur le lieu de travail, sous l'optique de cette finalité, que pour protéger les biens et les secrets de fabrication de l'entreprise contre la destruction, le vandalisme ou le vol, pour empêcher la divulgation d'informations confidentielles et pour garantir la sécurité et le bon fonctionnement du réseau informatique.

Elle retient que les termes « protection des biens » de l'entreprise ne justifient en revanche pas le contrôle de l'usage des outils informatiques visant à assurer la prévention, la recherche et la détection d'actes susceptibles d'engager la responsabilité de l'employeur et qui constituent une violation du règlement interne de l'entreprise ou des obligations contractuelles du salarié.

Les deux finalités reproduites ci-après invoquées par la requérante sont donc à écarter :

- *« La prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui (ex. : actes de piratage informatique, fuite de données relatives à la gestion du personnel ou de fichiers médicaux confidentiels, consultation de sites à caractère pornographique, pédophile, ou invitant à la discrimination raciale, ethnique, religieuse, etc.) ;*
- *Le respect de bonne foi des principes et règles d'utilisation des technologies en réseau de l'entreprise, notamment en vertu du règlement interne (ex. : abus des ressources de l'entreprise) ».*

Les finalités envisagées par la requérante représentent certes un intérêt légitime au sens de l'article 7 point f de la directive. Nécessité et légitimité constituent les critères de base de la licéité d'un traitement de données à caractère personnel qui doit par ailleurs respecter les qualités des données exigées par la directive (pertinence, proportionnalité…).

Aux termes du document WP 55 du groupe de travail « Article 29 » sur la protection des données concernant la surveillance des communications électroniques sur le lieu de travail, adopté le 29 mai 2002, le principe de légitimité signifie que toute opération de traitement de données ne peut être effectuée que si sa finalité est légitime au sens de l'article 7 de la directive et des dispositions de la législation nationale qui la transpose. L'article 7, point f de la directive s'applique particulièrement à ce principe, étant donné que, pour être autorisé en vertu de la directive 95/46/CE, le traitement des données d'un salarié doit être nécessaire à la réalisation de l'intérêt légitime poursuivi par l'employeur et ne pas entraver les droits fondamentaux des salariés.

S'il est vrai que les documents adoptés par le groupe institué par l'article 29 de la directive se réfèrent aux principes relatifs à la légitimation des traitements des données prévus à l'article 7 de la directive (et plus particulièrement à l'article 7 point f), principes que l'on retrouve en droit interne sous l'article 5 de la loi (dont plus particulièrement l'article 5, paragraphe 1er, lettre d) et qui recouvrent également la finalité indiquée par le requérant tendant à se protéger en termes de responsabilité civile ou pénale, il n'en reste pas moins que l'article 11 de la loi établit des règles spécifiques et exhaustives pour les traitements à des fins de surveillance sur le lieu du travail.

Ainsi le législateur luxembourgeois n'a pas retenu le critère général de l'intérêt légitime au sens de l'article 7 point f de la directive comme étant suffisant pour fonder une surveillance sur le lieu du travail, mais a tenu à le traduire dans une liste limitative des cas d'ouverture inscrite à l'article 11 paragraphe 1er de la loi.

La Commission nationale déjà en l'occasion de rendre attentif le gouvernement à cette situation qui découle très clairement de la volonté du législateur de 2002.

Il est vrai qu'il avait été envisagé dans la version initiale du projet de loi N°5181 d'ajouter à l'article 11 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, une condition de légitimité supplémentaire et spécifique « pour détecter les actes susceptibles d'engager la responsabilité de l'employeur quelque soit son statut, public ou privé » mais il se trouve que cet amendement a été retiré et que la loi n'a pas été complétée sur ce point.

Il en suit que seules deux des quatre finalités mentionnées dans la demande cadrent avec la condition de légitimité « protection des biens de l'entreprise » invoquée par la requérante et sont éligibles pour légitimer la surveillance électronique, à savoir :

- *La protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires (ex. : concurrence déloyale, divulgation de fichiers, violation des secrets d'affaire ou des droits de propriété intellectuelle de tiers, atteintes à l'image de marque de l'entreprise, etc.) ;*
- *La sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, y compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise (ex. : phénomènes d'engorgement, propagation de virus, etc.).*

C) Principes tenant à la qualité des données (article 4) :

> La Commission nationale rappelle qu'un traitement à des fins de surveillance (que ce soit le régime général visé à l'article 10 ou le régime particulier prévu à l'article 11) doit, pour être licite, être effectué conformément aux dispositions de l'article 4 de la loi (cf. document parlementaire 4735/13, p. 17).

Suivant l'article 4, paragraphe 1er de la loi, « le responsable du traitement doit s'assurer que les données qu'il traite le sont loyalement et licitement, et notamment que ces données sont :

(a) collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ;

(b) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ;

(c) exactes et, si nécessaire, mises à jour; toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;

(d) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées… ».

1) Le principe de finalité / le principe de nécessité

S'il est vrai que le traitement à des fins de surveillance sur le lieu de travail peut être mis en œuvre, conformément à l'article 14, il n'en demeure pas moins qu'aux termes de l'article 11, paragraphe 1er, alinéa 1er un tel traitement n'est possible que s'il est nécessaire.

« Avant de commencer toute surveillance, l'employeur doit s'assurer que cette surveillance est absolument nécessaire pour une finalité déterminée. Cette surveillance ne doit pas être continue et ne doit être envisagée que dans des circonstances exceptionnelles, comme par exemple, lorsque l'employeur doit protéger ses intérêts en cas d'activité criminelle développée par le salarié, ou pour assurer la sécurité du système (détection de virus).

L'activité de surveillance doit être gouvernée par la transparence, tant à l'égard des autorités et des salariés, voire même à l'égard des tierces personnes (par exemple, indication standard sur un courrier électronique adressé à une personne extérieure à l'entreprise que la réponse peut faire l'objet d'une mesure de surveillance). L'information des salariés doit être claire, précise et exacte. Les circonstances dans lesquelles la surveillance a lieu doivent être décrites avec précision, comme par exemple, les conditions dans lesquelles le matériel de l'entreprise peut être utilisé à des fins privées, les conditions de la surveillance (par qui, quand, comment), les conséquences qui pourraient être tirées des résultats de cette surveillance. » (cf. document parlementaire 4735/13, p. 22 et 23).

Rappelons que les finalités éligibles du traitement envisagé sont motivées par la requérante dans sa demande du 7 octobre 2003 de la manière suivante :

« Toujours dans son règlement interne, Odyssey a précisé que la Société se réservait le droit d'entreprendre des contrôles uniquement pour les raisons suivantes :

- *La protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires (ex. : concurrence déloyale, divulgation de fichiers, violation des secrets d'affaire ou des droits de propriété intellectuelle de tiers, atteintes à l'image de marque de l'entreprise, etc.) ;*
- *La sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, y compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise (ex. : phénomènes d'engorgement, propagation de virus, etc.) ».*

Il convient en outre de rapprocher ces deux finalités précitées avec la description détaillée des mesures de sécurité (prescrite aux articles 22 et 23 de la loi), telle que contenue dans la demande initiale du 7 octobre 2003 :

« Dans le règlement intérieur, afin de garantir un traitement approprié et équitable, les limites de la mise en œuvre des contrôles ont été clairement spécifiées :

- Des contrôles peuvent être effectués seulement sous la responsabilité de notre Auditeur interne, qui est aussi en charge de veiller au respect de la protection des données.
- Il peut y avoir deux types de contrôles :

  Suite à une plainte (exemple : un e-mail reçu par quelqu'un) ou s'il y a de fort soupçons sur les agissements d'un collaborateur (exemple : notre service IT constate que le disque personnel est entrain d'occuper une place très importante). Dès lors, ce dernier sera avisé personnellement et anticipativement qu'un contrôle aura lieu et celui-ci sera exécuté en sa présence.

  Dans le cadre des « Finalités du Traitement », des contrôles par échantillon pourront être opérés. Ils ne pourront pas excéder une période de 5 jours dans un mois et l'échantillon devra comprendre au minimum 5 personnes. Aucune donnée comportant la mention « privé » ne sera visionnée et l'approche se fera sous le mode « tatillon » (il est interdit de contrôler systématiquement toutes les données d'une personne ou / et de l'échantillon).

En ce qui concerne la protection des données, la gestion des accès est supervisée par le responsable du service concerné (à savoir, Responsable Finance, Responsable Ressources Humaines ou Responsable IT en fonction du type de données concernées) et chaque collaborateur possède son propre mot de passe. Nos lignes de communication interne sont cryptées. La boîte à lettre électronique est aussi protégée par un mot de passe (avec au minimum 8 caractères alpha numériques). L'espace disque personnel alloué à chaque collaborateur, n'est accessible que par ce dernier.

Les données des Ressources Humaines sont sous la responsabilité de ce département. Les dossiers de nos collaborateurs sont sauvegardés dans un coffre et les données électroniques sont gérées à travers une application Oracle, qui offre un niveau de sécurité garanti par le fournisseur.

Des sauvegardes sont régulièrement faites par notre service IT et les supports magnétiques sont stockés dans un coffre fort.

Enfin, notre règlement intérieur impose aux collaborateurs d'Odyssey le respect d'une série de mesures relatives à la sécurité du matériel mis à leur disposition et les données qu'ils seront amenés à traiter dans le cadre de leurs activités. »

a) Le secret des correspondances

La Commission nationale relève qu'il y a de distinguer deux catégories de courriers électroniques, les courriels personnels et les courriels professionnels. Les deux catégories sont certes toutes deux soumises au secret des correspondances privées mais en ce qui concerne les courriers professionnels, c'est l'entreprise elle-même qui doit être considérée comme destinataire, respectivement expéditrice.

En ce qui concerne les courriers personnels émis ou reçus par les salariés en nom personnel, l'employeur est tenu de ne pas violer le secret des correspondances privées. Il ne peut donc procéder à un contrôle des courriers électroniques personnels de ses employés que dans le cas où ces derniers auraient consenti préalablement à un tel contrôle conformément à la loi du 11 août 1982. Dans le cas contraire, l'employeur ne peut surveiller l'utilisation de la messagerie électronique de l'entreprise dans la mesure où cette surveillance porte atteinte au secret des correspondances privées.

En raisonnant par analogie à la jurisprudence rendue en matière de courrier postal, le caractère professionnel des « e-mails » devra être reconnu sur le lieu de travail en l'absence des mentions « privé » ou « personnel » dans le titre de ce dernier. Il existe donc une présomption du caractère professionnel des « e-mails » sur le lieu de travail. Ainsi, si un message est adressé au salarié sans que ne figure la mention « personnel » dans son objet, il est présumé avoir un caractère professionnel et peut dès lors être surveillé par l'employeur.

Au cas où tous les courriels (personnels et professionnels) sont mélangés dans la boîte de réception de la messagerie électronique de l'employé, il sera difficile d'avoir accès aux messages de l'entreprise au risque de violer à cette occasion la confidentialité des messages à caractère personnel.

b) La distinction entre les messages personnels et professionnels

Pour parer à ce genre de problème relatif à la distinction entre messages personnels et messages professionnels, la Commission nationale recommande à la requérante à demander que chaque e-mail personnel des salariés se signale comme tel dans son intitulé par une indication manifeste dans l'objet du message, voire à demander aux salariés de créer un « folder personnel » ou « répertoire personnel » dédié aux correspondances personnelles y archivées lui conférant ainsi le caractère et la nature d'une correspondance personnelle.

Concrètement, la requérante serait donc bien avisée, soit de faire mettre en place par leurs salariés une double boîte de messagerie permettant de distinguer les messages personnels et les messages professionnels, soit d'inviter ces derniers à classer les messages reçus dans un dossier identifié comme « personnel » ou « privé » lorsqu'ils présentent un tel caractère, et d'insérer sous cette optique dans les contrats de travail une clause suivant laquelle l'employé donnerait expressément son consentement à ce que son courrier électronique, reçu sur l'adresse électronique de l'entreprise (par opposition à une adresse de type "hotmail" personnelle de l'employé), sur l'ordinateur mis à sa disposition par l'entreprise, soit considéré comme étant le courrier de l'entreprise qui puisse être accédé par l'entreprise ou faire l'objet d'une surveillance de l'entreprise.

2) Le principe de proportionnalité

La surveillance doit être adaptée au but légitime poursuivi. L'employeur doit recourir aux moyens de surveillance les plus protecteurs de la sphère privée du salarié. Le respect de ce principe de proportionnalité exige que, par exemple, doivent être évitées les surveillances automatiques et continues des salariés. De même la surveillance du contenu des courriers électroniques peut être disproportionnée, alors que l'employeur peut se limiter à surveiller les temps d'utilisations, le nombre de courriers électroniques ou la taille des annexes. Des techniques permettent de limiter ou de bloquer l'accès à Internet. L'employeur doit également agir avec discernement et tenir compte des possibilités de réponses erronées de moteurs de recherche, de liens erronés ou de publicités trompeuses" (cf. document parlementaire 4735/13, p. 22 et 23).

« Tout contrôle devrait être ponctuel et justifié par des indices laissant suspecter une utilisation abusive des outils de travail. Un contrôle général et a priori de l'ensemble des données de télécommunications de même qu'un enregistrement systématique de l'ensemble de ces données apparaît disproportionné par rapport à l'objectif poursuivi. Il est en outre peu conforme à la dignité humaine - et pas nécessairement productif - de faire travailler des employés sous une surveillance constante. » (cf. Commission pour la protection de la vie privée, avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail du 3 avril 2000, numéro du rôle 10/2000).

- Quant au contrôle des enregistrements des fichiers de journalisation et du contenu des disques durs

L'employeur aura tendance à considérer que l'infrastructure informatique de l'entreprise lui appartient et qu'elle n'est mise à disposition des salariés et collaborateurs externes que pour les seules fins professionnelles. Un contrôle permanent et omniprésent serait donc justifié de manière absolue tant en raison du droit de propriété des outils utilisés que du rôle de direction de l'entreprise dont il a la responsabilité et du fait des obligations découlant du contrat de travail des salariés.

Tel n'est cependant pas le cas car la jurisprudence reconnaît désormais que les salariés doivent pouvoir bénéficier également sur leur lieu de travail et pendant les heures de travail payés par l'employeur d'une sphère résiduelle de vie privée les protégeant contre une surveillance excessive de la part de l'employeur.

Dans la mesure où les enregistrements des fichiers de journalisation et le contenu des disques durs et partitions attribués aux salariés, qui contiennent des données personnelles, sont exposés à une surveillance de la part de l'employeur, celle-ci doit être considérée comme excessive si elle prenait la forme d'une analyse nominative (salarié individuel identifié) sans graduation dans le rythme et l'envergure des données contrôlées.

En d'autres termes le contrôle permanent et omniprésent est certes admis pour les finalités légitimes répondant à des besoins de l'entreprise mais l'analyse des données ne doit être effectuée par référence aux salariés individuels concernés que de façon ponctuelle.

Ces vérifications ne peuvent être intensifiées graduellement qu'à l'égard de ceux des salariés individuels contre lesquels les vérifications ponctuelles ont dégagé des indices d'abus, d'utilisation illégitime des outils informatiques et moyens de communication électronique, mis à leur disposition ou de comportement déloyal envers l'entreprise.

Le principe de proportionnalité exige la limitation à une surveillance ponctuelle et le respect d'une graduation dans l'intensification de la surveillance (« Kontrollverdichtung ») qui doit être justifié chaque fois par des indices et soupçons préalablement détecté.

- Quant au courrier électronique

En ce qui concerne le courrier électronique la Commission nationale considère que la prise de connaissance systématique du contenu des courriers électroniques par l'employeur est à qualifier d'excessive, et serait contraire aux dispositions légales susmentionnées, de la même façon que le serait l'écoute et/ou l'enregistrement des communications téléphoniques de l'employé.

Il existe différentes solutions qui permettent de cibler les courriers suspects, tels que les logiciels qui identifient l'expédition de courriers électroniques en chaîne ou qui isolent et/ou bloquent ceux dont la taille est excessive et qui peuvent provoquer un engorgement ou un ralentissement du réseau. Ceci est le cas en particulier lorsque des images ou des fichiers exécutables sont envoyés ou reçus en annexe aux messages.

C'est ainsi sur la base d'une liste de courriers et non de leur contenu - comme par analogie en matière d'utilisation du téléphone sur la base des coûts de communication laissant apparaître des montants anormalement élevés - que le non-respect des règles posées par l'employeur pourra être décelée.

La Commission nationale ajoute que l'absence de respect desdites règles devrait être prise en considération par l'employeur au regard des courriers envoyés par l'employé, elle émet toutefois des réserves quant à l'exercice du contrôle au regard des courriers entrants, l'employé n'étant pas l'auteur de ces derniers (à l'exception des contrôles par le biais de moyens techniques, visant par exemple le blocage des courriers entrants multiples en comportant des pièces jointes de grande taille qui constituent un risque d'engorgement du réseau).

(cf. Commission pour la protection de la vie privée, avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail du 3 avril 2000, numéro du rôle 10/2000).

La Commission nationale relève que si l'employeur ne peut, à défaut d'avoir obtenu l'accord du salarié, contrôler le contenu des messages personnels, il pourra quand même en contrôler le volume, la fréquence, la taille, le format de leurs pièces jointes et le temps passé par le salarié à ces activités personnelles.

- Quant à la navigation sur Internet (contrôle des sites accédés)

En ce qui concerne la surveillance des sites Internet consultés par l'employé, les données concernées sont tant des données de trafic (adresse des sites consultés) que le cas échéant du contenu afférent. Ces données constituent des données à caractère personnel à partir du moment où l'employeur est en mesure d'établir un lien entre les adresses des sites consultés et un employé particulier.

Dans cette optique, la Commission belge est d'avis que le contrôle doit se fonder sur des données objectives restreintes et non sur une prise de connaissance préalable et systématique du contenu de toutes les données de trafic concernant chaque employé.

L'employeur pourra à cet effet disposer par exemple d'une liste d'adresses de sites consultés de façon globale sur une certaine période, sans que soient identifiés dans un premier temps les auteurs des consultations (surveillance non nominative). Il pourra sur cette base repérer une durée anormalement élevée de consultation d'Internet ou la mention d'adresses de sites suspects et prendre les mesures de contrôle appropriées (en passant seulement dans ce second stade à une surveillance nominative). La détection de la consultation de certains sites pourrait également être effectuée de façon automatique grâce à un logiciel spécifique sur la base de mots-clés déterminés.

(cf. Commission belge pour la protection de la vie privée, avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail du 3 avril 2000, numéro du rôle 10/2000).

a) Origine des données et catégories de données et traitements envisagés :

Dans sa demande, l'employeur expose :

« Les données qui seront principalement traitées sont celles provenant de :

1. la boîte à lettre électronique
2. les fichiers transmis et reçus
3. les disques durs de l'ordinateur et autres supports magnétiques.

Le traitement de ces données se fera dans le cadre de l'activité professionnelle et si nécessaire, dans un but de contrôles (selon les « finalités du traitement ») ».

La Commission nationale est d'avis qu'en l'espèce les mesures de surveillance décrites dans la demande sont adéquates et en proportion avec la finalité recherchée.

La Commission nationale estime que les catégories de données traitées et les modalités de mise en œuvre de la surveillance peuvent être considérées comme adéquates, pertinentes et non excessives par rapport à la finalité recherchée.

b) Catégories de personnes concernées :

Dans sa demande la requérante expose que sont concernés « tous les collaborateurs (employés) » et « les consultants externes effectuant une prestation pour le compte d'Odyssey et ayant accès au réseau interne d'Odyssey ».

c) Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées :

Seuls l'auditeur interne et le responsable des ressources humaines figurent comme destinataires.

Les catégories de destinataires mentionnées apparaissent aux yeux de la Commission nationale comme étant à la fois légitimes et proportionnées à la finalité poursuivie.

d) Durée de conservation des données :

Conformément à l'article 4, paragraphe 1, lettre (d) de la loi du 2 août 2002, les données traitées ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

Le stockage des données pendant une durée déterminée, par exemple sur un serveur de réseau, doit être effectué en conformité avec les dispositions des articles 21 à 23 de la loi du 2 août 2002 concernant la confidentialité et la sécurité des traitements. En particulier, l'accès à ces données ne peut être autorisé que par l'employeur et dans les conditions et pour les finalités strictes prévues pour l'exercice d'un contrôle. Il s'agit en effet d'éviter que des données qui peuvent s'avérer confidentielles ne puissent être interceptées par des personnes extérieures à la communication (par exemple échange de courriers électroniques entre membres d'un syndicat, documents préparatoires à une prise de position officielle d'une institution ou d'une entreprise, ou encore échange de vues confidentiel entre différentes entreprises ou autorités). (cf. Commission pour la protection de la vie privée, avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail du 3 avril 2000, numéro du rôle 10/2000).

La requérante a indiqué dans sa demande initiale du 7 octobre 2003 que les données seront conservées « selon les prescriptions légales ». Dans son second courrier du 16 mars 2004, elle a précisé que les données sont conservées durant toute la période active du collaborateur et qu'après le départ de celui-ci son dossier personnel est encore conservé pendant 10 années.

La Commission nationale estime que si dans certaines circonstances ce délai peut apparaître comme étant nécessaire et non excessif au regard de la finalité poursuivie, dans d'autres, la durée de conservation pourra être limitée à un délai plus court.

D) Pays tiers à destination desquels les transferts de données sont envisagées

Suivant la demande, un transfert de données vers un pays tiers (hors Union Européenne) n'est envisagé que vers la Suisse.

D'après une décision de la Commission de Bruxelles ce pays offre un niveau de protection adéquat au sens de l'article 18 de la loi du 2 août 2002.

La Commission nationale rappelle qu'en vertu du paragraphe 1er de l'article 18 précité « le transfert vers un pays tiers de données faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat et moyennant le respect des dispositions de la présente loi et de ses règlements d'exécution ».

Il en suit que le destinataire externe établi en Suisse ne peut traiter les données lui transférées en respectant les dispositions de la présente loi et de ses règlements d'exécution, en particulier les principes de finalité, de proportionnalité et de transparence y inscrits.

E) Mesures de sécurité prévues aux articles 22 et 23 de la loi

L'ensemble de ces mesures (de sécurité) doit conférer un „niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger" (cf. document parlementaire 4735/13 p.37 et Directive 95/46/CE, article 17, paragraphe 2).

Ces mesures doivent également viser à prévenir tout autre risque d'atteinte aux données tel que leur vol, leur effacement, etc., ainsi que tout risque d'utilisation pour d'autres finalités (cf. avis d'initiative relatif aux traitements d'images effectués en particulier par le biais de systèmes de vidéosurveillance, n° de rôle 34/99 du 13/12/1999 (Commission pour la protection de la vie privée, Belgique)).

En l'espèce, les mesures de sécurité prévues aux articles 22 et 23 de la loi ont fait l'objet d'une description détaillée dans le second courrier du 16 mars 2004 de la requérante.

La Commission nationale constate que le contenu de cette description satisfait aux exigences des prédits articles.

F) Mesures d'information

En ce qui concerne le droit à l'information de la personne concernée (articles 10(2), 11 (2) et 26 de la loi), la Commission nationale tient à rajouter que dans un souci de transparence le dialogue entre employeur et employés (et des tiers) devra permettre d'établir de façon suffisamment détaillée les différentes caractéristiques de la politique de contrôle de l'employeur. Celles-ci devront notamment viser :

- les modalités d'utilisation du courrier électronique et de l'Internet qui sont permises, tolérées ou interdites ;

- les finalités et modalités du contrôle de cette utilisation (nature des données collectées, étendue et circonstances des contrôles, personnes ou catégories de personnes sujettes aux procédures de contrôle (6)) ;

- l'existence d'un stockage des données de télécommunication et la durée de ce stockage, par exemple sur un serveur central, dans le cadre de la gestion technique du réseau, et les éventuels systèmes de cryptage existants ;

- les décisions pouvant être prises par l'employeur à l'endroit de l'employé sur la base du traitement des données collectées à l'occasion d'un contrôle ;

- le droit d'accès de l'employé aux données à caractère personnel le concernant.

(cf. Commission pour la protection de la vie privée, avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail du 3 avril 2000, numéro du rôle 10/2000).

PAR CES MOTIFS

La Commission nationale, réunissant deux de ses trois membres effectifs ainsi qu'un membre suppléant appelé en remplacement du membre effectif dûment empêché et délibérant à l'unanimité des voix,

se déclare compétente pour connaître de la demande d'autorisation du traitement à des fins de surveillance sur le lieu du travail introduite par la requérante ;

reçoit la demande d'autorisation en la forme ;

au fond, la déclare partiellement fondée ;

rejette la demande à défaut de condition de légitimité afférente prévue par la loi pour les finalités « prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui » et « respect de bonne foi des principes et règles d'utilisation des technologies en réseau de l'entreprise, notamment en vertu du règlement interne » ;

accueille la demande pour les finalités « protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires » et « sécurité et/ou bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, y compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise ».

partant, autorise la requérante à recourir aux mesures envisagées de surveillance des installations informatiques utilisées par son personnel et les collaborateurs externes ainsi que de leurs communications électroniques, selon les modalités précisées dans sa demande du 7 octobre 2003, complétée en date du 16 mars 2004, sous réserve de respecter les conditions suivantes :

1) Les communications, correspondances et messages électroniques personnels (caractérisés comme privés ou s'avérant de toute évidence comme étant étrangers à l'activité professionnelle) ne doivent pas être contrôlés, sauf ceux émanant ou destinés aux personnes physiques ayant préalablement marqué leur consentement individuel conformément à l'article 2 de la loi du 11 août 1982 concernant la protection de la vie privée.

2) Le personnel et les collaborateurs externes susceptibles d'être exposés à la surveillance de leur utilisation des outils informatiques et communications électroniques doivent en être préalablement informés par l'employeur conformément à l'article 10 paragraphe (2) en ce qui concerne les collaborateurs / tiers et à l'article 11 paragraphe (2) en ce qui concerne les salariés.

3) La surveillance devra être mise en œuvre dans le respect du principe de proportionnalité commandant l'absence de contrôle général et permanent, si ce n'est si celui-ci fait abstraction de toute analyse nominative et référence individuelle aux collaborateurs concernés. L'analyse individuelle et une identification du contrôle d'un collaborateur déterminé présupposent la constatation préalable d'indices de soupçons d'abus ou de comportement irrégulier portant atteinte aux intérêts économiques, commerciaux et financiers, à la sécurité des données et/ou au bon fonctionnement technique des systèmes informatiques et réseaux de l'entreprise.

4) plus généralement :

La requérante doit assurer que la mise en œuvre du traitement autorisé respecte à tout moment les principes de finalité et de loyauté inscrits dans la loi et les droits de la personne concernée visés au chapitre VI de la loi du 2 août 2002.

En ce qui concerne les deux derniers points la Commission nationale renvoie à l'excellent « Guide relatif à l'utilisation d'Internet et du courrier électronique sur le lieu de travail » publié par le Préposé fédéral suisse à la protection des données disponible à l'adresse Internet suivante :

http://www.edsb.ch/f/doku/leitfaeden/internet/internet.pdf

Ainsi décidé à Esch-sur-Alzette en date du 1ier juillet 2005

La Commission nationale pour la protection des données

(*s.*) Gérard Lommel	(*s.*) Pierre Weimerskirch	(*s.*) Thierry Lallemang
Président	Membre effectif	Membre effectif

Avis de la Commission nationale pour la protection des données concernant l'avant-projet de loi sur le contrôle des voyageurs dans les établissements d'hébergement et au projet de règlement grand-ducal relatif au modèle des fiches à tenir par les tenanciers d'établissements d'hébergement

Délibération n°84/2005 du 11 novembre 2005

Conformément à l'article 32, paragraphe 3, lettre (e) de la loi 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 entre autres pour mission d'« être demandée en son avis sur 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, et faisant suite à la demande lui adressée par le Ministère des Classes moyennes, du Tourisme et du Logement que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet de l'avant-projet de loi sur le contrôle des voyageurs dans les établissements d'hébergement et au projet de règlement grand ducal relatif au modèle des fiches à tenir par les tenanciers d'établissements d'hébergement.

1. L'identification du responsable du traitement

Selon l'article 2, lettre (o) de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après : la loi du 2 août 2002), « lorsque les finalités et les moyens de traitement sont déterminés par ou en vertu des dispositions légales, le responsable du traitement est déterminé par ou en vertu des critères spécifiques conformément aux dispositions légales ». Or, l'identité du responsable du traitement ne ressort pas explicitement de cet avant projet de loi.

La Commission nationale propose d'insérer une disposition dans l'avant-projet de loi telle que « le responsable du traitement des données à caractère personnel effectué dans le cadre de la présente loi est X ».

Il ne fait pas de doute que le logeur est le responsable du traitement pour la collecte et la transmission des données à la Police et au Statec de la fiche d'hébergement. Il n'en reste pas moins que la Police et le Statec poursuivent leurs propres finalités et sont responsables de leurs propres traitements. A défaut d'apporter cette précision, il risque d'avoir des confusions dans la compréhension des paragraphes (1) (l'identification du responsable du traitement) et (5) (le respect de l'article 17 de la loi du 2 août 2002) alors qu'il y est également question de responsable de traitement.

2. Les finalités de la fiche d'hébergement

L'article 4, paragraphe (1), lettre (a) de la loi du 2 août 2002 exige notamment que les données doivent « être collectées pour des finalités déterminées, explicites et légitimes (…) ». La Commission nationale recommande de détailler les finalités du traitement pour chacun des trois acteurs différents, à savoir le logeur, la Police et le Statec.

A titre d'exemple, pourrait-on préciser que la finalité du traitement pour le logeur serait de répondre à une exigence légale, outre l'intérêt qu'il pourrait y trouver pour les besoins de la gestion de sa clientèle notamment la connaissance de sa clientèle, celle de la Police serait la répression des infractions sur le territoire nationale, notamment en matière de séjour des étrangers et celle du Statec serait d'avoir des données statistiques fiables afin de recenser et d'étudier l'évolution des flux touristiques et/ou d'étudier la compétitivité économique de la branche touristique.

3. Le principe de nécessité et l'accès du Statec à la fiche originale

Aux termes de la loi du 2 août 2002, la collecte des données ne doit pas aller au-delà de ce qui est nécessaire au regard de la finalité poursuivie. Or, si l'article 2 du règlement grand-ducal (ci-après : RGD) précise que le Statec reçoit certaines informations limitativement énumérées (données dépersonnalisées) figurant sur la fiche d'hébergement, la loi prévoit que le Statec peut accéder à l'intégralité de la fiche originale et ce, sans restrictions (article 4 de l'avant-projet de loi).

La Commission nationale se demande si ces deux dispositions se contredisent sans que les raisons de cette contradiction résultent clairement des explications des commentaires des articles. Elle considère aussi qu'il n'est pas nécessaire que le Statec ait accès à toutes les informations de la fiche originale. Compte tenu de la mission qui lui incombe des données dépersonnalisées devraient suffire. Dès lors, il serait préférable d'un point de vue de la protection des données que le Statec ne reçoive que les informations qui figurent dans la fiche qui lui est transmise par le logeur. L'on peut cependant se poser la question s'il ne suffirait pas simplement de rajouter aux informations transmises au Statec une indication concernant la provenance géographique du voyageur, sans qu'il ne soit pour autant nécessaire que le Statec ait accès aux autres coordonnées personnelles du voyageur.

4. Le respect du principe de légitimité

Pour être légitime, le traitement de données relatif à la fiche d'hébergement doit satisfaire à l'un des critères fixés à l'article 5 de la loi du 2 août 2002.

Pour le logeur, la Commission nationale suggère que le traitement soit légitimé sur base de l'article 5, paragraphe (1), lettres (a) et/ou (d). En effet, en vertu de ladite lettre (a), un traitement est légitime s'il « est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ». Sur base de la lettre (d), « le traitement [doit être] nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement (…) » ; cet intérêt légitime est son activité hôtelière.

Pour la Police et le Statec, la légitimité repose sur l'article 5, paragraphe (b) puisque le traitement envisagé est « nécessaire à l'exécution de [leur] mission d'intérêt public » (par exemple, la prévention des infractions, l'impact du secteur touristique dans l'économie nationale).

5. Le respect de l'article 17 de la loi du 2 août 2002

L'article 17, paragraphe (1), lettre (a), dispose que « font l'objet d'un règlement grand-ducal les traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions pénales qui sont réservés, conformément à leurs missions légales et réglementaires respectives, aux organes du corps de la police grand-ducale (…) ». Il ne fait pas de doute que le traitement de la Police rentre dans l'hypothèse ci-avant décrite.

La Commission nationale estime qu'il n'est pas nécessaire qu'un règlement grand-ducal séparé soit pris à cet effet, le règlement grand-ducal pris en exécution du projet de loi relatif à la fiche d'hébergement et qui est annexé à l'avant-projet, pouvant valablement intégrer ces exigences.

A cette fin ledit règlement grand-ducal devra déterminer conformément à l'article 17 exige que « le responsable du traitement, la condition de légitimité du traitement, la ou les finalités du traitement, la ou les catégories de personnes concernées et les données ou les catégories de données s'y rapportant, l'origine de ces données, les tiers ou les catégories de tiers auxquels ces données peuvent être communiquées et les mesures à prendre pour assurer la sécurité du traitement en application de l'article 22 de la présente loi ». A cet effet, les développements sous les points 1, 2 et 4 pourront utilement aider.

Dans le cadre des mesures de sécurité (cf. point 7 ci-après), la Commission nationale suggère de prévoir que l'identifiant de l'agent ayant procédé à une interrogation, ainsi que la date, l'heure, l'objet du traitement et le motif de chaque interrogation soit toujours enregistrés. Ces données ne devraient être accessibles, à des fins de contrôle, qu'aux membres de l'autorité de contrôle institué par l'article 17, paragraphe (2) de la loi du 2 août 2002, ainsi qu'au Directeur général de la Police ou aux agents nommément désignés par lui et à l'Inspecteur général de la Police.

6. Quant à la préservation et le respect des droits des personnes concernées

Le chapitre IV de la loi du 2 août 2002 est entièrement consacré aux droits de la personne concernée (en l'espèce, le voyageur) : il s'agit du droit à l'information (article 26), du droit d'accès et de rectification (article 28) aux données la concernant ainsi que du droit d'opposition (article 30). L'exercice de ces droits offre à la personne concernée la possibilité de jouer un rôle actif dans le respect de la protection des données et de contrôler les traitements dont ils font l'objet.

Afin d'assurer le respect des droits de la personne concernée, la Commission recommande d'insérer un texte afférent en bas de chaque fiche d'hébergement signée par le voyageur. Cette information au voyageur pourrait recevoir la teneur suivante :

« *Le voyageur est informé que les données à caractère personnel qui lui sont demandées et collectées sont nécessaires en vertu de la loi du xxx. Conformément à la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement de données à caractère personnel, le voyageur dispose à tout moment auprès du logeur d'un droit d'accès et de rectification des données le concernant.*»

Il convient de remarquer que l'article 29 de la loi du 2 août 2002 prévoit des exceptions au principe du droit d'accès, notamment en matière de prévention et de poursuites des infractions et de sûreté de l'Etat. La Police grand-ducale peut ainsi limiter ou différer le droit d'accès de la personne concernée. Dans ce dernier cas, si le voyageur voulait exercer son droit d'accès, il devrait passer par l'intermédiaire de la Commission nationale.

Enfin, la question du droit d'accès du voyageur à la fiche transmise au Statec ne se pose pas, dès lors que ce dernier n'est censé recevoir que des données dépersonnalisées.

7. Le problème de la conservation des données et les mesures de sécurité

Conformément à l'article 4, paragraphe (1) lettre (d) de la loi du 2 août 2002, les données traitées ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant la durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées. La Commission estime qu'un délai de trois ans est proportionné par rapport aux finalités poursuivies. Le logeur traite la fiche originale signée par le voyageur, de sorte qu'il est logique qu'il soit chargé de la conservation des données.

De plus, en vertu des articles 22 et 23 de cette même loi, des mesures de sécurité de nature organisationnelle et technique doivent être prises pour éviter tout risque d'atteinte aux données (par exemple effacement des données, la diffusion ou l'accès non autorisés). Tant les fichiers tenus par le logeur que ceux de la Police et du Statec devront être conformes à ces prescriptions. La Commission nationale suggère d'inscrire également des dispositions afférentes dans le règlement grand-ducal en particulier en ce qui concerne la transmission des données.

La Commission nationale soulève aussi que selon l'article 2 in fine du règlement grand-ducal, quand le logeur choisit le système des fichiers électroniques, il devrait encore l'imprimer sur un papier carton : il y aurait pourtant un double emploi d'un même fichier, ce qui n'a aucun intérêt, d'autant plus que cela augmente le risque de porter atteinte à la sécurité des données.

8. Observations purement formelles

En dehors du contexte de la protection des données, la Commission nationale se permet de vous rendre attentif aux observations purement formelles suivantes :

- Aux termes de l'article 1er du RGD, le modèle de fiche d'hébergement doit être rédigé en langues française, anglaise, allemande et néerlandaise. Or, le modèle de la fiche d'hébergement n'est pas traduit en néerlandais.
- L'article 2 du RGD n'énumère pas l'intégralité des mentions devant figurer sur la fiche d'hébergement. Font en effet défaut les mentions relatives au numéro de la pièce d'identité présentée ainsi que le numéro d'immatriculation du véhicule.
- Enfin, le dernier paragraphe de l'article 2 n'est pas clair : il est en effet difficile de connaître précisément les informations qui figurent sur cette fiche. Il est simplement écrit que la fiche remise à la Police aura les « mêmes informations » sans toutefois préciser s'il s'agit des mêmes informations que celles de la fiche originale ou celles de la fiche transmise au Statec, la phrase précédente énumérant en effet les informations transmises au Statec. La Police devant détenir l'intégralité des informations figurant sur la fiche originale, et dans un souci d'éviter toute confusion, il faudrait insérer la dernière phrase de cet article 2 entre les deux derniers paragraphes.

Ainsi décidé à Luxembourg en date du 11 novembre 2005

La Commission nationale pour la protection des données

(*s.*) Gérard Lommel	(*s.*) Pierre Weimerskirch	(*s.*) Thierry Lallemang
Président	Membre effectif	Membre effectif

Avis de la Commission nationale pour la protection des données concernant le projet de loi portant modification de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et des articles 5 paragraphe (1) lettre a) ; 9 paragraphe (1) lettre a) et 12 de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 23 paragraphe (2) points 1. et 2. de la loi du 8 juin 2004 sur la liberté d'expression dans les médias.

Délibération n°85/2005 du 5 décembre 2005

Par courrier du 21 novembre 2005, Monsieur le Ministre délégué aux Communications a bien voulu soumettre pour avis à la Commission nationale le projet de loi prémentionné, à l'élaboration duquel elle a été associée, en lui demandant de lui faire part d'éventuels commentaires substantiels résiduels.

I. Considérations générales

Dans son rapport d'activité pour l'année 2003 et le 1er trimestre 2004 adressé au gouvernement en août 2004, la Commission nationale exprimait son insatisfaction de ne pas être matériellement en mesure de traiter les demandes d'autorisation introduites dans des délais raisonnables et faisait part de sa constatation que l'attention des responsables de fichiers et de traitements de données restait trop focalisée sur l'accomplissement des formalités préalables prévues au chapitre III.

Elle préconisait dès lors une simplification substantielle du régime de déclaration des traitements et un allègement des formalités administratives, allant jusqu'à encourager le gouvernement à envisager de restreindre les traitements de données et cas de figure nécessitant l'autorisation préalable conformément à l'article 14.

Elle souhaitait également voir apporter certaines clarifications dans le texte de la loi ainsi que des modifications susceptibles d'aligner le droit luxembourgeois sur le texte de la directive chaque fois que les écarts n'apparaissaient pas réellement nécessaires ou suffisamment justifiés pour compenser les difficultés d'interprétation et d'application de la loi auxquels ils donnent souvent lieu.

L'intention du gouvernement de procéder rapidement à une révision de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel annoncée solennellement dans le programme de coalition avec comme objectif primaire de clarifier et de simplifier les procédures de façon à éliminer certains obstacles purement administratifs sans plus-value pour la protection de la vie privée et les libertés individuelles, était donc enregistrée avec beaucoup de satisfaction par la Commission nationale pour la protection des données qui annonçait elle-même vouloir dorénavant mettre davantage l'accent sur ses missions de guidance des responsables de traitements et d'explication de la loi, d'information et, le cas échéant, de contrôle a posteriori plutôt que d'examen des formalités administratives préalables.

Le texte du présent projet de loi procède de cette façon de voir les choses et résout un grand nombre de difficultés actuelles.

Un puissant coup de gouvernail n'était sans doute pas nécessaire, un démantèlement des mécanismes de protection actuels aurait été ressenti comme indéfendable, mais des retouches, clarifications et simplifications susceptibles de faciliter l'application de la loi et de surcroît de désengorger la Commission nationale pour la protection des données étaient hautement souhaitables, y compris certaines modifications au régime applicable aux traitements à des fins de surveillance des articles 10 et 11.

Nous sommes profondément convaincus que la loi doit à la fois être claire et assurer une protection efficace des citoyens. Les formalités administratives n'ont de sens que si elles facilitent l'application des dispositions de la loi.

Celle-ci ne devrait pas être plus ambitieuse que ce qu'on peut raisonnablement espérer voir être appliqué en pratique par les entreprises, les administrations et organisations et autres professionnels normalement diligents.

Des règles de protection qui restent lettres mortes se retournent en pratique contre la crédibilité et l'efficacité du cadre légal et contre celles de l'autorité chargée de veiller à son application.

Pour ces raisons, la Commission nationale pour la protection des données accueille favorablement les modifications proposées dans le projet de loi, y compris certains assouplissements dont elle est convaincue qu'ils sont indispensables pour permettre qu'elle soit mieux respectée et donc renforcer la rigueur de son application.

Dans cet esprit elle a estimé devoir formuler dans les développements qui suivent quelques propositions supplémentaires notamment concernant le régime des traitements à des fins de surveillance dont elle espère qu'elles s'avèreront adoptées aux besoins et possibilités effectives.

Nous nous félicitons donc de l'approche générale de l'avant-projet de loi consistant à apporter les clarifications nécessaires et à simplifier les formalités préalables à la mise en œuvre des traitements (chapitre III) sans réduire pour autant le niveau général de la protection légale.

Comme Monsieur le Ministre délégué aux Communications l'a fait remarquer lors de la conférence de presse de la Commission nationale pour la protection des données le 25 octobre 2004, la priorité doit revenir à l'établissement et à l'amélioration d'une culture de la protection de la vie privée et des données personnelles au Grand-Duché (l'important est que cela rentre dans les mentalités, pas seulement sur les formulaires).

Ceci concorde avec la vision stratégique de notre Commission nationale qui, à l'instar de ses consoeurs plus prestigieuses dans d'autres Etats membres, entend dorénavant se concentrer de façon privilégiée à l'information du public, l'élaboration d'avis et de recommandations, la guidance des responsables de traitements de données et la promotion des meilleures pratiques en la matière.

II. Allègement de la procédure de déclaration des traitements

L'élargissement des exemptions de l'obligation de notification des traitements prévue aux articles 12 et 13 est de nature à répondre non seulement aux souhaits exprimés dans la prise de position du groupe patronal du Comité national pour la simplification administrative en faveur des entreprises, mais suit également les préconisations par le groupe de travail européen des commissaires à la protection des données (Groupe article 29) dans son rapport relatif à la simplification de l'obligation de notification et d'un meilleur usage des exemptions permises par la directive 1.

Le groupe européen des commissaires à la protection des données s'est en effet déclaré favorable à l'introduction d'un éventail plus large d'exemptions dans les législations nationales pour dispenser de la formalité administrative les traitements de données les plus courants qui ne sont normalement pas susceptibles de porter atteinte à la sphère privée des individus.

Bien que le catalogue des exemptions de l'obligation de notification qu'il est proposé de rajouter à l'article 12 soit bien moins volumineux que les exemples analysés par le groupe patronal du CNSAE dans son papier de réflexion, les cas d'ouverture sont décrits de façon plus large et générale de sorte que dans l'application pratique l'impact de la modification proposée devrait se rapprocher de celui du décret afférent pris au Pays-Bas dont le texte s'étend tout de même sur 76 pages.

[1] WP 106 du 18 janvier 2005 ; (http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp106_en.pdf

Les Pays-Bas ont également repris dans leur législation de façon optionnelle pour les responsables de fichiers et traitements l'institution du détaché à la protection des données comme cas d'exemption de l'obligation de notification. Le rapport du Groupe de l'article 29 relate en outre les expériences positives faites en Allemagne, puis en Suède et aux Pays-Bas avec l'institution du chargé de la protection des données propre à l'établissement (betrieblicher Datenschutzbeauftragter) comme alternative à l'obligation de notification.

Cette exemption qui a également été introduite il y a un an dans la loi française figure déjà dans la loi du 2 août 2002 comme une faculté optionnelle pour les responsables du traitement.

Le chargé de la protection des données

Il n'y a pas d'obligation pour le responsable du traitement de nommer un tel chargé de la protection des données. Le responsable du traitement aura peut-être intérêt à le faire, alors que ce chargé peut se substituer dans certains cas à la Commission nationale et qu'il peut, mieux que la Commission nationale, car plus près du responsable du traitement, conseiller et guider celui-ci dans l'application des dispositions du présent projet de loi. La subsidiarité et parfois la complémentarité du chargé par rapport à la Commission nationale devront permettre de limiter « l'ampleur bureaucratique du contrôle ».2

Il résulte d'une récente note de synthèse publiée par la CNIL sur les détachés à la protection des données et intitulée « Étude comparée sur les détachés à la protection des données (DPOs) désignés par les responsables de traitement en application de l'article 18 paragraphe 2 de la Directive 95/46/EC3 » que le premier bilan dans les cinq pays de l'Union européenne ayant opté pour ce régime de simplification est globalement positif. Il s'est en effet avéré que le recours au chargé de la protection dans nos pays voisins a indéniablement contribué à diminuer la bureaucratie, à renforcer une meilleure diffusion de la culture de la protection de la vie privée et à développer l'autorégulation dans divers secteurs d'activité.

A. L'élargissement du cercle des personnes pouvant être désignées comme chargé de la protection des données

Jusqu'à présent le chargé de la protection des données ne peut être salarié du responsable du traitement. Cette incompatibilité avait été jugée nécessaire par le législateur en 2002 pour suffire au critère d'indépendance requise par la directive.

L'assouplissement du dispositif, en permettant à l'avenir également à un salarié du responsable du traitement d'assurer la mission du chargé de la protection des données, rendra ce régime encore plus attractif. Il va sans dire que le chargé de la protection des données doit exercer son jugement en dehors de toute pression et présenter ses conclusions sans parti pris, du fait qu'il aura à apprécier la licéité de traitements portant, par exemple, sur la surveillance de l'activité du personnel ou qu'il aura pour devoir de préconiser des solutions organisationnelles ou technologiques qui pourraient ne pas recueillir immédiatement l'assentiment de sa hiérarchie ou des services concernés.

Conformément à l'article 18 de la directive européenne 95/46/CE (repris au paragraphe 3 de l'article 40 de la loi), le détaché doit pouvoir exercer ses fonctions en toute indépendance. Plusieurs éléments ont été identifiés par les États membres pour traduire l'exigence d'indépendance posée dans la directive.

- La liberté d'action du chargé de la protection des données

  Le positionnement hiérarchique ou encore la possibilité pour le détaché d'en référer directement au responsable de traitement sont retenus comme critères-clés de son indépendance. La loi allemande prévoit ainsi que le détaché doit être rattaché directement au directeur de la société ou de l'organisation.

- L'absence de conflit d'intérêts

[2] cf. document parlementaire 4735/13, p. 38.
[3] http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CIL/dpo-comparaison-UE-VD.pdf

Il est évident que le détaché ne doit pas voir son jugement altéré en raison d'autres fonctions qu'il exercerait parallèlement. L'indépendance dans l'exercice de ses missions implique également qu'il ne puisse être amené à se contrôler lui-même.

- En Allemagne

Cette notion de « conflit d'intérêt » est au cœur du choix du « Datenschutzbeauftragter » (ci-après « DSB ») en Allemagne, où une incompatibilité stricte en a été déduite avec des fonctions de direction de l'organisme. Des conflits d'intérêt ont également été relevés lorsque le DSB occupe également des fonctions dans les domaines ayant trait à la gestion des ressources humaines, à l'administration des systèmes d'information, aux technologies de l'information, ainsi que tout département mettant en oeuvre des traitements de données sensibles ou de grande envergure (par exemple : marketing).

L'absence de conflit d'intérêt s'apprécie au cas par cas et, en Allemagne, les autorités de contrôle compétentes, saisies le plus souvent par des salariés, interviennent régulièrement pour obtenir, à l'amiable ou sous la contrainte, la décharge du DSB ne remplissant pas ou plus cette exigence.

- En France

La notion de conflit d'intérêts a aussi été reprise dans la réglementation française, « les fonctions ou activités exercées concurremment par le correspondant ne doivent pas être susceptibles de provoquer un conflit d'intérêts avec l'exercice de sa mission ».4

L'indépendance du correspondant français est renforcée par le fait qu'il « ne reçoit aucune instruction pour l'exercice de sa mission ». La législation française prévoit un devoir de collaboration active à charge du responsable du traitement, que le correspondant soit salarié ou non. Le texte allemand va dans le même sens.5

Il est à relever que le système français du correspondant à la protection des données à caractère personnel, introduit par un décret n° 2005-1309 du 20 octobre 2005, prévoit un régime qui rappelle le statut du travailleur désigné, tout en rajoutant quelques dispositions supplémentaires intéressantes :

- obligation de porter la désignation d'un correspondant à la connaissance des représentants du personnel ;
- le correspondant exerce sa mission directement auprès du responsable du traitement et ne dispose donc pas d'autre supérieur hiérarchique ;
- le correspondant ne reçoit aucune instruction dans l'exercice de sa mission ;
- la fonction de correspondant et de responsable de traitement ou son représentant légal ne peuvent être cumulées ;
- les fonctions ou activités exercées concurremment par le correspondant ne doivent pas être susceptibles de provoquer un conflit d'intérêts ;
- le responsable du traitement doit collaborer activement à la mission du correspondant ;

---

[4] cf. article 46 du décret n° 2005-1309 du 20 octobre 2005 (J.O n° 247 du 22 octobre 2005); http://www.cnil.fr/index.php?id=1880

« Art. 46. Le correspondant à la protection des données à caractère personnel exerce sa mission directement auprès du responsable des traitements.

Le correspondant ne reçoit aucune instruction pour l'exercice de sa mission.

Le responsable des traitements ou son représentant légal ne peut être désigné comme correspondant.

Les fonctions ou activités exercées concurremment par le correspondant ne doivent pas être susceptibles de provoquer un conflit d'intérêts avec l'exercice de sa mission. »

[5] « *Die öffentlichen und nicht-öffentlichen Stellen haben den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen*. »

- le correspondant doit établir un bilan annuel qui doit être présenté au responsable de traitement et à la Commission ;

La loi allemande rajoute encore quelques éléments intéressants, qui ne se retrouvent pas dans le texte français :

- ne peut être désignée DSB qu'une personne particulièrement qualifiée ;
- le DSB ne doit pas subir de préjudice ou de désavantage en raison de l'exercice de ses fonctions ;
- obligation à charge du responsable du traitement de collaborer avec le DSB et de lui fournir tous les moyens nécessaires à l'exercice de ses fonctions (locaux, effectifs, etc.).

Les idées les plus importantes ont été reprises dans le projet de loi par l'ajout de 2 alinéas à l'article 40 paragraphe (3) et l'insertion d'un paragraphe (4).

Il nous paraît toutefois indiqué de proposer au gouvernement d'envisager quelques modifications complémentaires pour parfaire le régime juridique s'appliquant au chargé de la protection des données:

- il peut être utile d'ajouter que le chargé n'agit pas sur instruction du responsable, mais gère indépendamment sa mission.

  Cette précision aurait le mérite d'être plus claire et directe que le seul fait d'affirmer l'indépendance du chargé.

- le responsable du traitement doit collaborer avec le chargé et doit mettre à sa disposition tous les moyens nécessaires à l'exécution de sa mission.

  L'absence d'une telle disposition risquerait d'encourager des entreprises d'entraver l'exercice de la mission en gardant une attitude complètement passive.

- finalement, on peut également s'interroger sur l'opportunité de créer une sanction spécifique à l'encontre de l'employeur en cas de violation de ces dispositions.

III. Le régime de l'autorisation préalable

Quant au régime de l'examen préalable (correspondant à l'article 20 de la directive), un resserrement du nombre des traitements de données qui doivent faire l'objet d'une autorisation, conformément à l'article 14 de la loi, avant leur mise en œuvre se justifie non seulement pour des raisons pratiques (en vue d'aboutir à un désengorgement de la Commission nationale pour la protection des données) mais est également conforme à l'esprit de la directive et à la tendance générale observée ces dernières années dans les autres Etats membres.

Au vœu du considérant 54, le nombre de ceux (traitements de données) présentant des risques particuliers (au regard des droits et des libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités ou du fait de l'usage particulier d'une technologie nouvelle) devrait être très restreint.

Ainsi la loi française, à l'instar de celles d'autres pays, ne soumet également à l'examen préalable de la CNIL le traitement de données sensibles que dans certains cas de figure.

En revanche elle prévoit ce régime renforcé notamment pour (Article 25 de la loi française) :

1) certains traitements de données sensibles

2) les traitements portant sur des données génétiques

3) ceux portant sur les infractions et condamnations pénales, sauf s'ils sont mis en œuvre par les auxiliaires de justice dans le cadre de leurs missions

4) les traitements susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire (effet discriminatoire)

5) l'interconnexion de fichiers dont les finalités sont différentes

6) les traitements portant sur des données parmi lesquelles figurent le numéro d'inscription des personnes ou répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire

7) les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes

8) ceux comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

L'avant-projet de loi s'inspire de ce catalogue de la loi française à l'exception des points 3), 6) et 7).

Au sujet du point 6) ci-dessus, la Commission nationale profite de l'occasion pour rappeler au gouvernement la nécessité de procéder à une révision de la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales et le répertoire afférent et se réfère à ce sujet à ses observations exprimées dans le cadre de son avis relatif au projet de règlement grand-ducal pris en exécution de la loi du 11 novembre 2003 relative à la publicité foncière6.

L'évolution récente fait apparaître que les conditions prévues par la loi du 30 mars 1979 ne sont plus respectées dans bien des cas et que ce texte ne répond plus à l'exigence de l'article 8 paragraphe 7 de la directive 95/46/CE du 24 octobre 1995 sur la protection des données personnelles qui dispose que les Etats membres déterminent les conditions dans lesquelles un numéro national d'identification peut faire l'objet d'un traitement.

Pour le surplus, les modifications et clarifications proposées dans l'avant-projet de loi concernant les données sensibles (articles 6 et 7), les traitements réalisés dans le cadre de la liberté d'expression (article 9), à la surveillance (articles 10 et 11), à l'interconnexion de données (article 16), les traitements relatifs au crédit et à la solvabilité des personnes (article 14) et au régime de l'autorisation préalable lui-même recueillent l'adhésion des membres de la Commission nationale.

Nous considérons toutefois que quelques assouplissements supplémentaires se justifieraient dans un souci de réalisme et d'adaptation du cadre légal à ce qui pourra être appliqué rigoureusement au jour le jour, et donc en fin de compte, de crédibilité de la loi.

A. Le régime des traitements à des fins de surveillance

Il résulte des travaux parlementaires que le législateur entendait mettre en place un cadre légal assez restrictif pour la mise en œuvre des traitements de données à des fins de surveillance et cela aussi bien pour ceux opérés par l'employeur à l'égard de ses salariés sur le lieu de travail (article 11) et que pour ceux exercés par tout autre responsable du traitement envers des tiers (article 10).

Cette volonté d'instituer une protection efficace7 s'est accompagnée du souci que les dispositions adoptées soient claires et assurent dans l'intérêt de toutes les parties en cause la sécurité juridique nécessaire puisqu'elles sont assorties de sanctions pénales. Elle s'est traduite pour ces types de traitements par une dérogation à l'article 5 qui définit les causes légitimes d'un traitement de données à caractère personnel en reprenant celles de l'article 7 de la directive.

Conformément au considérant 30 de la directive les Etats membres peuvent préciser dans leur loi nationale quand l'intérêt légitime du responsable du traitement ou bien les libertés et droits fondamentaux de la personne concernée prévaut en particulier dans le cadre des activités légitimes de gestion des entreprises et autres organisations.

---

6 Avis de la Commission nationale pour la protection des données 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, délibération N°2/2004 du 9 janvier 2004

7 (Doc. parlem. 4735[13] page 19)

La dérogation retenue consistait à insérer dans le texte des articles 10 et 11 une énumération limitative des conditions de légitimité qui doivent être réunies pour rendre la surveillance et le traitement des données afférentes licites, les cas d'ouverture étant décrits de façon plus précise que dans les critères de légitimation généraux de la directive auquel il n'est dérogé cependant que dans le but de la clarification et de la sécurité juridique (sinon il y aurait transposition incorrecte de la directive).

Par ailleurs, le consentement des personnes concernées est exclu comme critère de légitimation d'une surveillance des salariés sur leur lieu de travail mis en œuvre par l'employeur.

Cette approche très rigoureuse répond à la grande sensibilité du public à l'égard du recours à des moyens techniques pour contrôler les allers et venues et les comportements des citoyens, en particulier s'ils sont mis en œuvre dans les lieux publics, accessibles au public et sur le lieu de travail.

Le régime légal des traitements à des fins de surveillance continue à donner lieu à certaines critiques alors qu'une autorisation préalable est requise dans tous les cas énumérés tant à l'article 10 qu'à l'article 11 et que ces catalogues ne prévoient parfois pas de cas d'ouverture permettant d'autoriser des mesures de surveillance dans des circonstances ou pour un but déterminé que l'entreprise, l'administration ou l'organisation considère toutefois comme suffisamment graves pour les légitimer.

Les organisations représentatives des employeurs[8] ont tendance à qualifier les choix opérés par le législateur dans le libellé des articles 10 et 11 comme trop restrictifs et comme ne tenant pas assez compte de l'évolution des techniques et pratiques professionnelles et notamment de la nécessité pour l'employeur qui assure la responsabilité économique de l'exploitation de l'entreprise et de sa pérennité (y compris les incidences sociales) et auquel revient dès lors le pouvoir de direction dans celle-ci, d'avoir les moyens de combattre la fraude, l'usage illégitime des équipements informatiques et d'Internet, de détecter les actes contraires à la loi ou aux bonnes mœurs qui sont susceptibles d'engager la responsabilité de l'employeur ou de lui causer un préjudice économique ou financier.

L'option retenue par le législateur (catalogue détaillé énumérant exhaustivement les cas d'ouverture qui seuls sont reconnus comme légitimes) qui privilégie la protection des personnes et la clarté et prévisibilité de la règle juridique comporte par nature le risque de lacunes dans cette liste limitative et de rigidité de son application.

La Commission nationale pour la protection des données a certes la latitude de nuancer son appréciation de la nécessité et de la proportionnalité des mesures de surveillance envisagées au regard de la finalité poursuivie en fonction du cas de figure précis, des circonstances, du contexte et de suivre dans sa politique l'évolution des pratiques et des mœurs.

Au niveau de la vérification de la légitimité elle ne peut toutefois pallier à l'absence de critère de légitimation et doit toujours se référer à une condition de légitimité expressément prévue dans le texte des articles 10 et 11 pour justifier la délivrance d'une autorisation.

Les trois premières années d'expérience d'examen des dossiers ont permis à la Commission nationale de mettre en évidence une lacune dans les conditions de légitimité de l'article 10 qui s'est traduite par de nombreux cas d'impossibilité de délivrer une autorisation (pour la mise en place d'une vidéosurveillance), notamment pour combattre le vol à l'étalage ou le vandalisme alors que la protection des biens (pourtant prévue à l'article 11) y fait défaut[9].

Par ailleurs, le cas de figure prévu à l'article 11 paragraphe (1) lettre (d) donne lieu à des difficultés d'interprétation et d'application.

[8] cf. papier de réflexion du groupe patronal au sein du CNSAE du 12 juillet 2005 relatif à la réforme et simplification de certaines dispositions de la loi du 2 août 2002 sur la protection des données

[9] cf. Cyril Pierre-Beausse. La Protection des données personnelles (éditions Promoculture 2004) N°171 : « Un cas d'ouverture manquant : La surveillance des biens ».

Nous notons en outre que la condition de légitimité supplémentaire qu'il était prévu dans la version initiale du projet de loi N°5181 (devenue la loi du 30 mai 2005 relative aux dispositions spécifiques de protection des personnes à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques) de rajouter à l'article 11 de la loi du 2 août 2002 « pour assurer la prévention, la recherche et la détection d'actes susceptibles d'engager la responsabilité de l'employeur » ne se retrouve pas dans l'avant-projet de loi10.

Tenant compte de tous ces éléments et de l'expérience acquise à ce jour par notre Commission nationale, qui n'arrive malheureusement pas à évacuer dans des délais raisonnables les nombreux dossiers de demandes d'autorisation dont elle est saisie, nous considérons qu'il est possible et souhaitable de voir étendre au régime des articles 10 et 11 de la loi visant les traitements à des fins de surveillance certes de façon mesurée et circonspecte l'effort d'assouplissement et de simplification des formalités administratives à charge des responsables de traitement sans affecter sensiblement le niveau de protection assuré par la loi.

Il apparaît qu'au niveau européen une grande majorité des pays ne disposent pas de cadre légal à portée générale en matière de surveillance sur le lieu du travail. Certes, il est communément admis que la législation relative à la protection des données y trouve application11, ce qui donne cependant fréquemment lieu à des difficultés d'interprétation. Certaines législations européennes règlent des aspects spécifiques comme par exemple le contrôle par l'employeur de l'usage des courriers électroniques et de la navigation sur Internet ou le recours à la vidéosurveillance.

Enfin, la plupart des pays européens reconnaissent aux organes représentatifs certains droits ou pouvoirs en rapport avec la mise en place et/ou l'utilisation de système de surveillance par l'employeur12.

En ce qui concerne la vidéosurveillance, seuls deux pays européens prévoient dans leur législation-cadre relative à la protection des données un examen préalable à la mise en œuvre d'un système de surveillance par caméras, à savoir le Portugal, sous certaines conditions, et le Luxembourg. Dans un certain nombre d'Etats membres13 (l'Allemagne, le Danemark, l'Espagne, la France, les Pays-Bas, le Portugal, la Suède et l'Autriche) des législations spécifiques ont été prises pour réglementer la vidéosurveillance, mais elles ont la plupart du temps un champ d'application limité (p.ex. limité aux lieux publics ou ouverts au public). Parmi elles, certaines requièrent des autorisations administratives (p.ex. vidéosurveillance des espaces publics en France ou en Suède).

Il convient de se rendre compte que la loi luxembourgeoise assure une protection triplement renforcée des personnes à l'égard de traitements de données à des fins de surveillance par rapport au régime de la directive 95/46/CE du 24 octobre 1995 qu'elle transpose par les spécificités suivantes :

- catalogue restreint et détaillé des conditions de légitimité éligibles
- examen préalable par la Commission nationale pour la protection des données dont l'autorisation requise tient compte également de la balance des intérêts en cause (nécessité et proportionnalité des mesures de surveillance envisagées)
- exclusion du consentement des salariés comme critère de légitimation d'une surveillance mise en œuvre par l'employeur sur le lieu de travail.

---

10 Voir aussi Cyril Pierre-Beausse : ouvrage prémentionné N°190 : « Un cas d'ouverture manquant : la mise en cause de la responsabilité du responsable du traitement ».

11 Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel adopté le 13 septembre 2001 par le Groupe de travail « Article 29 »; doc. WP48 ; http://europa.eu.int/comm/justice_home/fsj/privacy/docs/ wpdocs/2001/wp48fr.pdf

12 cf. tableau comparatif, annexe 1

13 cf. résumé synthétique, annexe 2

Sur 1100 demandes introduites entre le 1er janvier 2003 et 31 juin 2005 plus de 800 (72%) portent sur des traitements à des fins de surveillance dont une très forte proportion est destinée à s'exercer au moins partiellement à l'égard des salariés (dans des proportions à peu près équivalentes sous forme de vidéosurveillance (182) surveillance de l'usage de la messagerie électronique, de l'ordinateur et d'Internet (139), surveillance des horaires de travail (131), contrôle d'accès des bâtiments (122) et surveillance des conversations téléphoniques (y compris enregistrement) (120)).

B. Modifications proposées

Article 10 : Traitements à des fins de surveillance

1ère Proposition : insérer au paragraphe 1er à la fin de l'alinéa (b) le texte suivant :

- « … à la protection des biens du responsable du traitement ou d'un tiers pourvu que le lieu présente de par sa nature, sa situation, sa configuration ou sa fréquentation un risque caractérisé d'acte de vandalisme ou de vol, ou… »

Commentaire : il s'agit de rajouter une condition de légitimité supplémentaire pour la mise en œuvre de traitements à des fins de surveillance (la plupart du temps par caméras vidéo) visant à endiguer des actes de vandalisme ou de vol.

Il apparaît incohérent que la protection des biens de l'entreprise figure parmi les critères de légitimation d'une surveillance mise en œuvre par l'employeur à l'égard de ses salariés sur le lieu de travail (article 11 paragraphe 1 lettre (b)) alors que l'autorisation afférente ne peut pas être accordée pour la surveillance de tiers, si ce n'est en cas de nécessité pour la sécurité (physique) des usagers ou la prévention d'accidents.

S'il ne s'agit pas en l'espèce d'un simple oubli du législateur, le texte actuel de la loi est en décalage manifeste avec des pratiques largement répandues – y compris dans notre pays – et acceptées par le public découlant de la constatation, que dans certains cas une surveillance (notamment par caméras vidéo) peut être nécessaire même en l'absence de risques pour l'intégrité physique des personnes, mais pour prévenir et réduire des actes de vandalisme et des vols fréquents et importants. Encore faut-il que la prolifération de ces dispositifs soient juridiquement encadrée et limitée.

Il y a lieu de noter que la rédaction proposée requiert la justification d'un risque caractérisé et que le pouvoir d'appréciation laissé à la Commission nationale pour la protection des données lui permettra donc d'écarter les dossiers dans lesquels les circonstances ne font pas apparaître une nécessité effective et importante ou laissent subsister des doutes quant au caractère excessif (principe de proportionnalité) du traitement envisagé.

2ème Proposition : limiter les traitements à des fins de surveillance énumérés à l'article 14 paragraphe (2) comme soumis à l'autorisation préalable de la Commission nationale à ceux prévus à l'alinéa (b) du paragraphe 1er de l'article 10.

Commentaire : La modification proposée tend à restreindre les traitements à des fins de surveillance prévus à l'article 10 soumis à l'examen préalable de la Commission nationale pour la protection des données à ceux visés à la lettre (b).

Il nous paraît en effet défendable de se contenter de la formalité de la notification préalable à la mise en œuvre pour les mesures de surveillance pour lesquelles le responsable du traitement a obtenu le consentement des personnes concernées (article 10 paragraphe 1er lettre (a)) et pour celles qu'il entend exercer pour sécuriser les lieux d'accès privé où il est domicilié (ou établi). Les règles de fond applicables resteraient inchangées.

Le critère de légitimation continuera à être requis.

Les doutes quant à la licéité du traitement (apparus à l'examen des notifications) et les abus éventuels relevés par les personnes concernées pourront déclencher des investigations dans le cadre du contrôle a posteriori exercé par la Commission nationale pour la protection des données de sa propre initiative ou sur plainte d'une personne concernée et déboucher le cas échéant sur des sanctions.

L'obligation du responsable du traitement d'informer les personnes concernées au sujet de la surveillance opérée conformément aux articles 10 paragraphe 2 et 26 la transparence, reste elle aussi obligatoire et assortie de sanctions pénales.

Par contre le nombre de dossiers de demandes d'autorisation de traitements à des fins de surveillance devrait diminuer sensiblement et de ce fait réduire les délais de traitement des formalités administratives qui encombrent actuellement la Commission nationale.

Signalons que dans le cadre des travaux préparatoires14 de la réforme de la loi française (loi du 4 août 2004) sur l'Informatique et les Libertés, un amendement visant à soumettre à l'autorisation préalable de la CNIL « tout traitement relatif à la vidéosurveillance » a été rejeté et que les rapporteurs du Sénat (M. Alex Turk) et de l'Assemblée nationale (M. Francis Delattre), respectivement Président et membre de la CNIL, ont émis tous les deux un avis défavorable au motif qu'il ne serait « pas nécessaire ni pensable de soumettre au système d'autorisation préalable toutes les vidéosurveillances qui se mettent actuellement en place dans le pays ».

La vidéosurveillance des espaces publics en revanche y fait l'objet d'une loi spéciale et requiert l'autorisation du préfet prise après avis d'une commission départementale présidée par un magistrat de l'ordre judiciaire.

A notre avis les cas de figure visés à l'alinéa (b) du paragraphe 1er de l'article 10 sont ceux où l'appréciation de la balance des intérêts en cause et des critères de nécessité et de proportionnalité est la plus délicate à opérer et justifie dès lors pour des motifs de sécurité juridique et de protection des personnes, l'exigence d'une autorisation préalable.

Article 11 : Traitements à des fins de surveillance sur le lieu de travail

Proposition : diviser l'alinéa (d) du 1er paragraphe de l'article 11 en deux points distincts et rajouter une référence à la lettre (f) dans le 2ème alinéa du 1er paragraphe du même article visant les pouvoirs du Comité mixte :

« d) pour le contrôle de la production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte. La surveillance peut seulement être exercée de façon permanente si l'ingérence dans la vie privée des travailleurs est réduite au minimum.

f) pour le contrôle temporaire de l'activité et des prestations du travailleur lorsqu'une telle mesure est nécessaire :

- pour assurer la prévention, la recherche et la détection d'actes illicites ou susceptibles d'engager la responsabilité de l'employeur, ou
- pour la protection des intérêts économiques, commerciaux ou financiers de l'employeur, ou
- pour des besoins de formation des travailleurs ou pour l'évaluation et l'amélioration de l'organisation du travail, ou … »

Commentaire :

14 http://ameli.senat.fr/amendements/2001-2002/203/Amdt_101.html (amendement de Monsieur Bret/1ère lecture)

http://ameli.senat.fr/amendements/2003-2004/285/Amdt_8.html (amendement de Monsieur Bret/2ème lecture)

http://www.senat.fr/seances/s200407/s20040715/s20040715002.html#int1177 (compte rendu intégral des débats au sénat 2ème lecture/15 juillet 2004)

http://www.assembleenationale.fr/12/cri/2003-2004/20040205.asp#P158_8086 (compte rendu intégral des débats à l'assemblée 2ème lecture/29 avril 2004)

http://www.assembleenationale.fr/12/pdf/cri/2003-2004/cahiers/c20040205.pdf (amendements pour la séance du 29 avril 2004)

Ad lettre (d) : Le cas de figure visé par le texte actuel de l'article 11 paragraphe 1er lettre (d) nécessite presque toujours que le moyen technique de contrôle soit actif en permanence, sinon comment assurer que les éléments recensés soient exacts et complets pour calculer la rémunération.

La Commission nationale ne peut donc pas se baser sur ce cas d'ouverture pour autoriser un traitement à des fins de surveillance visant à opérer un contrôle continu et permanent des prestations des travailleurs (aucune autorisation n'a encore été accordée sur son fondement). Le critère de légitimation prévu par le législateur s'avère en fin de compte inopérant en pratique. Pour cette raison nous estimons nécessaire de supprimer l'exigence que le contrôle ne s'exerce que de façon temporaire sur les travailleurs.

Certes, l'idée qu'une surveillance, visant à évaluer le comportement et les performances du salarié, ne doit jamais être que ponctuelle ou temporaire reflète la politique des autorités nationales de surveillance compétentes dans les autres pays en matière de protection des données.15

Pour cette raison, il est proposé d'ajouter une condition supplémentaire (l'ingérence dans la vie privée des travailleurs devra être réduite au minimum) pour restreindre le nombre de cas où les travailleurs pourront être exposés à une surveillance en continu.

Prenons pour exemple un travailleur spécialisé d'une usine de faïencerie dont la fonction consiste à apposer la décoration sur les pièces de vaisselle en porcelaine en fabrication et qui est payée à la pièce. Assurément un contrôle ponctuel ne permettra pas de déterminer sa rémunération exacte, l'identification et le comptage des pièces fabriquées n'étant pas assurés de façon complète et fiable.

Un mécanisme technique intégré à la chaîne de fabrication qui détermine de façon automatique le nombre de tasses (assiettes, sous-coupes,…) décorées peut s'avérer adapté aux besoins (un cliquet assurant le comptage des pièces) de la détermination automatique des éléments de la rémunération tout en n'affectant que faiblement la sphère privée de la travailleuse.

Par contre une surveillance par caméra vidéo ne devrait pas être autorisée dans le même but, du moins si le travailleur se trouve en plein champ de vision, car il est généralement admis que les travailleurs ne peuvent être – sauf cas exceptionnels (caissiers d'une banque) – exposés à travailler en permanence sous le contrôle de caméras.

Rappelons ici à toutes fins utiles qu'une jurisprudence constante admet depuis quelques années que le salarié a le droit au respect de sa vie privée, y compris sur son lieu de travail pendant le temps de travail16, et qu'il est parfois difficile de démêler dans son activité et son comportement sur le lieu de travail ce qui relève de la vie privée et de sa fonction professionnelle.

L'employeur ne peut donc exiger le droit de contrôler (notamment par les moyens techniques modernes) dans le détail et à tout instant, l'ensemble de l'activité de ses salariés.

Par ailleurs, le droit à la protection de la vie privée et des données personnelles lui commande de privilégier les moyens de surveillance les moins intrusifs.

La Commission nationale examine cet aspect dans chaque dossier de demande d'autorisation et s'est vu amener souvent à soumettre le traitement à des conditions spécifiques.

---

15 - Avis 8/2001 (WP 48) du 13 septembre 2001 du Groupe de l'Article 29 sur les traitements de données à caractère personnel dans le contexte professionnel (http://www.europa.eu.int/comm/ justice_home/fsj/ privacy/docs/wpdocs/2001/wp48fr.pdf).
- La cybersurveillance des salariés (http://lesrapports.la documentationfrancaise.fr/BRP/044000175/0000.pdf);
- Document guide de l'autorité suisse relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail (http://www.edsb.ch/f/doku/leitfaeden/internet/index.htm).

16 Cour européenne des Droits de l'Homme : affaire Niemietz c/ Allemagne, 16 décembre 1992
Cour de cassation française, Chambre sociale : - Arrêt Nikon du 2 octobre 2001 et
- Arrêt NAMS du 10 novembre 2005

Le fait de préciser dans ce cas d'ouverture de l'article 11 (le seul qui pourrait donner lieu à une surveillance continue et permanente) que l'ingérence dans la vie privée des travailleurs doit être réduite à un minimum ne constitue donc qu'un rappel du principe de proportionnalité qui doit être appliqué au contenu des données et aux opérations de traitement des données personnelles envisagés.

Ad Nouvelle lettre (f) : Concernant l'article 11, les travaux parlementaires de la loi du 2 août 2002 s'étaient basés principalement sur la convention collective de travail N°68 relative à la surveillance par caméras sur le lieu de travail17 applicable en Belgique.

Le législateur avait voulu arbitrer en faveur d'une forte protection des travailleurs et d'une sécurité juridique dont bénéficieraient en fin de compte toutes les parties en cause, en soumettant tous les traitements par l'employeur à l'égard de ses salariés à l'examen préalable de la Commission nationale et en adoptant un catalogue précis et limitatif de conditions de légitimité.

Nous pensons que cette démarche très protectrice doit être maintenue pour que la surveillance automatisée/électronique ne devienne pas omniprésente sur les lieux de travail, l'employeur gardant par ailleurs toutes les prérogatives découlant de son pouvoir de direction de l'entreprise (ou de l'organisation) qui est la contrepartie de sa responsabilité économique et sociale, mais il devra l'exercer généralement par les moyens traditionnels de la gestion de ses ressources humaines et de son organisation.

[17] et http://www.cnt-nar.be/CCT/cct-68.doc

En revanche les arguments que le groupe patronal a fait valoir dans le cadre du CNSAE se recouvrent partiellement avec des difficultés et hésitations éprouvées également par la Commission nationale pour la protection des données dans l'application de la loi au cours de sa jeune expérience de l'examen de ces dossiers (les plus nombreux parmi les demandes d'autorisation).

Nous estimons en effet qu'il subsiste des circonstances non couvertes par le catalogue restrictif des cas d'ouverture énumérés à l'article 11 et qu'il est possible de le compléter sans dénaturer l'esprit de la loi en s'inspirant de ladite convention collective belge et de celle N°81 relative au contrôle des communications électroniques en réseau18 adoptée le 26 avril 2002 et également d'application généralisée en Belgique.

La formulation du nouvel alinéa (f) proposé se limite donc à reprendre certains cas d'ouverture figurant dans ces textes belges qui aux yeux de la Commission nationale peuvent justifier dans certains cas la mise en place de dispositif de surveillance. Il reste pourtant très limitatif, afin de ne pas trahir l'esprit du législateur de 2002. Il y a lieu de garder à l'esprit que la Commission nationale pour la protection des données ne peut accorder d'autorisation que dans les cas où la loi prévoit une condition de légitimité.

Quand tel est le cas, elle a en outre l'obligation de scruter consciencieusement la demande pour se rendre compte si les critères de nécessité et de proportionnalité sont bien remplis.

Compléter le texte de l'article 11 par l'ajout d'un certain nombre de conditions de légitimité supplémentaire ne reviendra donc pas à déclencher une avalanche de nouveaux traitements à des fins de surveillance sur le lieu de travail.

- pour assurer la prévention, la recherche et la détection d'actes illicites ou susceptibles d'engager la responsabilité de l'employeur

Une telle condition de légitimité correspond au souci de nombreux employeurs de s'assurer que l'utilisation sur le lieu du travail d'Internet par son personnel ne dépasse pas certaines limites généralement fixées dans le règlement intérieur d'entreprise ou dans une « charte informatique » spécifique.

- pour la protection des intérêts économiques, commerciaux ou financiers de l'employeur

Ce critère de légitimation a été inclus dans la convention collective belge pour justifier notamment une surveillance reconnue nécessaire pour éviter la divulgation déloyale de secrets d'affaires ou d'autres renseignements internes confidentiels.

- pour des besoins de formation des travailleurs ou l'évaluation et l'amélioration de l'organisation du travail

Plusieurs demandes d'autorisation de traitements envisagés avec ces finalités ont dû être refusées par le passé à défaut de cas d'ouverture prévu par le législateur. Notons cependant qu'une autorisation n'est concevable pour ce type de traitements (p.ex. ciblé sur le respect des mesures de sécurité au travail) qu'à des conditions très restrictives, en particulier s'ils sont limités dans un laps de temps extrêmement court et que les personnes concernées aient été informées au préalable de façon exhaustive.

La Commission ne manquera sans doute pas de poursuivre sa politique très réservée et prudente en matière de délivrance d'autorisations afférentes aux employeurs. Rappelons finalement que la loi pose en outre l'accord du Comité mixte comme préalable à la décision de mise en œuvre d'un tel traitement de données à des fins de surveillance sur le lieu de travail (dans les entreprises ou établissements où un tel organe existe).

[18] http://www.cnt-nar.be/CCT/cct-81.doc

Article 14 : Autorisation préalable de la Commission nationale

Proposition : remplacer à l'article 14 paragraphe (1) la teneur de la lettre (b) par le texte suivant :

« les traitements à des fins de surveillance visés :

- à l'article 10 paragraphe (1) lettre (b) dès lors que les données résultant de la surveillance font l'objet d'un enregistrement et à l'article 11 de la présente loi. »

Commentaire : Cette proposition est déjà commentée sous l'article 10 à la page 12

IV. Autres modifications

Article 6 paragraphe 2 lettre (a) et paragraphe 3 lettre (d) (Qualification du consentement)

L'article 8 paragraphe 2 lettre (a) de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel définit le consentement de la personne concernée de façon plus restrictive lorsqu'il doit légitimer une exception au principe d'interdiction du traitement des données dites « sensibles ». Le consentement implicite est exclu du fait que la directive rajoute l'adjectif « explicite » au terme consentement. Nous proposons d'aligner la teneur de la loi au libellé de la directive.

Proposition : insérer à l'article 6 paragraphe (2) lettre (a) ainsi qu'au paragraphe (3) lettre (d) premier alinéa du même article chaque fois après le mot « consentement », le terme « explicite »

Commentaire : Compte tenu des modifications apportées à la définition du « consentement » à l'article 2 lettre (c), il est indiqué d'ajouter le terme « explicite » aux endroits indiqués à l'article 6, afin que la loi soit pleinement conforme aux exigences de l'article 8 de la Directive 95/46/CE.

Dans le domaine des traitements de données par les services de santé il appartiendra au règlement grand-ducal prévu au paragraphe (4) de l'article 7 de préciser dans quelles circonstances le consentement est requis comme garantie appropriée supplémentaire et s'il doit à son tour être explicite.

En effet les cas de figure visés (médecine préventive, diagnostics médicaux, administration de soins et traitements, recherche scientifique, gestion des services de santé) sont basés sur des finalités limitativement énumérées et des conditions de légitimité propres indépendantes du consentement de la personne concernée (sauvegarde de l'intérêt vital, obligation légale, mission d'intérêt public respectivement nécessité découlant de l'exécution d'un contrat auquel la personne concernée est partie).

Articles 26 à 31 : Droits de la personne concernée

La Commission nationale pour la protection des données se félicite des modifications opérées au niveau des droits de la personne concernée visés par les articles 26 et 31 de la loi qui consistent à améliorer la clarté des dispositions afférentes respectivement dans leur alignement sur le texte de la directive. Elle estime cependant nécessaire de réitérer ici un point soulevé déjà dans son avis relatif au projet de loi sur la liberté d'expression dans les médias à propos du droit à l'information.

Article 9 paragraphe 1er lettre (c)

Proposition :

- Supprimer le point (c) de l'article 9 et renuméroter les points subséquents.
- Ajouter un 2ème paragraphe avec la teneur suivante :

« Lorsque des données sont collectées directement auprès de la personne concernée, le responsable du traitement peut, par dérogation à l'article 26 paragraphe 1er, lettres (b) et (c), se limiter à indiquer la finalité générale poursuivie par le traitement mis en œuvre aux seules fins de journalisme ou d'expression artistique ou littéraire. »

Commentaire : Déjà dans son avis au sujet du projet de loi N°4910 sur la liberté d'expression dans les médias[19], la Commission a tenu à rendre attentif le gouvernement que l'exception de l'obligation d'informer la personne concernée du traitement de ses données à caractère personnel et de lui indiquer notamment la finalité poursuivie prévue à l'article 9 paragraphe 1er lettre (c) de la loi du 2 août 2002 déjà dans sa teneur actuelle pour l'hypothèse où l'application du principe générale aurait pour conséquence de compromettre la collecte des données ou la publication peut déboucher sur une collecte déloyale de données (contraire à l'article 4 paragraphe 1er lettre (a)) dans l'hypothèse où les données sont recueillies directement auprès de la personne concernée.

La Commission nationale avait estimée que le texte actuel de l'article 9 paragraphe 1er lettre (c) qui devait être reproduit à l'article 68 de la loi sur la liberté d'expression dans les médias ouvrait grandement la porte à des abus et devait être modifié.

En effet, si en questionnant une personne sur des informations se rapportant à elle, à son comportement et à sa vie privée ou professionnelle, le journaliste n'aura pas à signaler qu'il recueille ces renseignements dans le cadre de son activité professionnelle et à des fins de publication, il y a de grands risques (et dans certains cas il pourra même se croire autorisé par la loi, voire encouragé à mentir délibérément) de voir la personne questionnée induite en erreur sur l'objet et le but de l'entretien de façon à l'inciter à faire des confidences qu'il n'aurait pas faite s'il était conscient des fins envisagées par les questions de son interlocuteur. Une telle façon de procéder serait de toute évidence contraire à la bonne foi et à l'exigence du traitement loyal et licite des données à caractère personnel posé comme un des principes de base de la loi dont il n'y a pas de justification d'exempter les responsables de traitements effectués dans le cadre de la liberté d'expression (pas plus que d'autres) ce qui pourrait d'ailleurs être considéré comme une transposition incorrecte de la directive.

[19] Délibération N°6bis/2003 du 17 octobre 2003 pages 16 à 18

Cette proposition de texte est équilibrée et constitue un compromis entre les intérêts contradictoires existant en la matière :

- d'un côté, le responsable du traitement ne serait pas contraint d'indiquer avec précision les finalités déterminées, ou fournir d'autres informations supplémentaires (ce qui est le cas des traitements tombant sous le coup du droit commun inscrit à l'article 26 de la loi du 2 août 2002),
- d'un autre côté, il devrait quand même informer la personne concernée qu'il entend opérer des traitements de données lui relatives aux seules fins de journalisme (ou d'expression artistique ou littéraire), ceci afin de minimiser d'emblée les risques d'abus.

Ainsi décidé à Luxembourg en date du 5 décembre 2005

La Commission nationale pour la protection des données

(*s.*) Gérard Lommel	(*s.*) Pierre Weimerskirch	(*s.*) Thierry Lallemang
Président	Membre effectif	Membre effectif

Tableau comparatif
Réglementations concernant les traitements de données à caractère personnel sur le lieu du travail dans les différents pays européens (examen de 14 pays)

Pays	Législation générale sur la protection des données à caractère personnel	Réglementation spécifique concernant la protection des données sur le lieu du travail
Allemagne	- Loi fédérale du 14 janvier 2003 sur la protection des données (transposant la Directive 95/46/CE). - Deux lois de 1997 dans le secteur des télécommunications « Teledienstdatenschutzgesetz, TDDSG » et « Telekommunikationsgesetz, TKG »	Les lois TDDSG et TKG de 1997 contiennent des restrictions en matière de surveillance lorsque l'employeur permet l'usage des e-mails et d'Internet à des fins privés. La loi « Betriebsverfassungsgesetz » accorde aux représentants du personnel un droit de co-décision sur les codes de conduites sur l'usage des e-mails et d'Internet à des fins privés et sur l'utilisation de moyens techniques destinés à surveiller le comportement et les performances des travailleurs.
Autriche	Loi fédérale de 2000 sur la protection des données (transposant la Directive 95/46/CE)	L'article 96 de la loi « Arbeitsverfassungsgesetz » prévoit l'accord obligatoire des organes de représentations du personnel pour l'installation de systèmes de surveillance susceptibles d'affecter la dignité des travailleurs.
Belgique	Loi du 8 décembre 1992, modifiée le 11 décembre 1998 sur la protection de la vie privée (transposant la Directive 95/46/CE)	- Convention collective de travail n°68 (16.06.1998) relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail - Convention collective de travail n° 81 (26.04.2002) relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communications électroniques en réseau
Danemark	Loi du 31 mai 2000 sur le traitement des données à caractère personnel (transposant la Directive 95/46/CE)	La loi de 1982 sur la vidéosurveillance s'applique également à la surveillance sur le lieu du travail (information

		des salariés). Des dispositions du Code pénal relative au secret des e-mails s'appliquent aux e-mails sur le lieu du travail
Espagne	Loi du 13 décembre 1999 sur la protection des données (transposant la Directive 95/46/CE)	Le Code du travail soumet l'introduction d'un système de surveillance sur le lieu de travail à un avis préalable des organes de représentation du personnel.
Finlande	Loi du 22 avril 1999 sur la protection des données (transposant la Directive 95/46/CE	Loi du 1er octobre 2001 sur la protection des données dans le contexte professionnel. Les représentants du personnel ont un droit de coopération en matière de surveillance et concernant l'usage des e-mails et d'Internet.
France	Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	Le Code du Travail dispose que les droits des personnes et les libertés individuelles et collectives ne peuvent pas être restreintes à moins que ce soit justifié par la nature de la tâche à accomplir et proportionné au but recherché. Obligation de l'employeur d'informer les salariés sur les traitements à des fins de surveillance
Grèce	Loi du 1997 sur la protection des données (transposant la Directive 95/46/CE)	Une directive de l'autorité de contrôle interprète la loi-cadre sur la protection des données en vue de l'appliquer au contexte professionnel.
Irlande	Loi de 1988, modifiée en 2003, sur la protection des données (transposant la Directive 95/46/CE)	/
Italie	Code de protection des données du 30 juin 2003 (transposant la Directive 95/46/CE)	Une loi (No. 300/70) sur le statut des travailleurs interdit l'usage de moyens techniques (y compris les nouvelles technologies) en vue de contrôler les activités des travailleurs
Pays-Bas	Loi du 6 juillet 2000 sur la protection des données (transposant la directive 95/46/CE)	Le consentement des organes de représentation du personnel est obligatoire en ce qui concerne l'usage des moyens de surveillance destinés à contrôler la présence, le comportement ou

		les performances des travailleurs. (article 27.1 de la loi relative aux organes de représentation du personnel)
Portugal	Loi du 26 octobre 1998 sur la protection des données (transposant la Directive 95/46/CE)	La loi sur le contrat de travail réglemente indirectement la surveillance par l'employeur du contenu des e-mails des travailleurs et l'utilisation de l'Internet par ceux-ci
Royaume-Uni	Loi de 1998 sur la protection des données (transposant la Directive 95/46/CE)	Le « Regulation of Investigatory Powers Act » de 2000 autorise les employeurs de surveiller et d'enregistrer des communications, sans le consentement des personnes concernées dans plusieurs hypothèses (p.ex. fournir la preuve d'une transaction commerciale ; prévenir et détecter les crimes ; rechercher ou détecter l'usage non autorisé du système de télécommunication).
Suède	Loi de 1998 sur la protection des données (transposant la Directive 95/46/CE)	La loi sur la co-décision prévoit que d'importants changements sur le lieu de travail (y compris en matière de surveillance) doivent être négociés entre l'employeur et les syndicats.

Résumé synthétique des législations des pays européens en matière de vidéosurveillance

1. Dispositions spécifiques relatives à la vidéosurveillance contenues dans les différentes législations nationales sur la protection des données des pays-membres[20].

Selon les différentes textes nationaux sur la protection des données, il apparaît que seulement le Luxembourg et le Portugal[21] ont spécifiquement prévu dans leurs lois respectives des obligations d'examen ou d'autorisation préalable par l'autorité de contrôle.

Ainsi il ressort de l'article 14 (1) (a) de la loi luxembourgeoise du 2 août 2002 sur la protection des données à caractère personnel, qu'une autorisation préalable aux fins d'une vidéosurveillance doit obligatoirement être demandée auprès de la Commission nationale.

Il ressort de l'article 28 (1) (a) de la loi portugaise du 26 octobre 1998, renvoyant à l'article 8 paragraphe 2 de ladite loi qu'un contrôle préalable et donc une autorisation de la CNPD doit être obtenue pour un traitement de données relatif à «… des soupçons d'activités illicites, délits, infractions administratives, décisions infligeant des peines, mesures de sécurité, amendes et sanctions accessoires… ».

Il convient de noter que des autorisations préalables sont également nécessaires aux fins d'une vidéosurveillance en France, en Espagne et en Suède. Dans ces trois cas de figure, il s'agit cependant de textes spécifiques portant sur la vidéosurveillance exclusivement, ces dispositions ne découlent d'aucune façon de la législation sur la protection des données à caractère personnel.

En France, il faut une autorisation préalable de la préfecture du lieu d'installation du système de vidéosurveillance[22] afin de pouvoir opérer une vidéosurveillance (i) sur la voie publique ou (ii) dans les lieux ouverts au public.

En Espagne, il faut une autorisation préalable de l'administration des « forces et corps de sécurité » pour toute installation d'un système de vidéosurveillance, par des personnes du secteur privé ou public.

En Suède, la vidéosurveillance « générale » requiert en principe l'autorisation d'une commission administrative régionale[23], mais il existe cependant un certain nombre d'exceptions, p.ex. la surveillance des bureaux de poste, des banques et des magasins. La vidéosurveillance secrète (enquêtes criminelles) doit être autorisée par un tribunal[24].

Toutes les autres législations des pays-membres ont prévu soit un mécanisme de déclaration préalable ou de notification préalable, soit elles sont muettes sur une telle mesure, tel p.ex. l'Allemagne.

Le champ d'application des législations spécifiques sur la vidéosurveillance.

Les pays suivants se sont dotés de lois ou règlements spécifiques portant exclusivement sur la vidéosurveillance : l'Allemagne, le Danemark, l'Espagne, la France, les Pays-Bas, le Portugal, la Suède et l'Autriche. Il faut aussi citer l'Italie et le Royaume-Uni qui, à part les lois ou règlements spécifiques en la matière, ont également adopté des codes de conduite.

Les dispositions législatives spécifiques de l'Allemagne, l'Espagne, la France, la Suède et de l'Autriche ne portent que sur la vidéosurveillance dans des lieux publics (et parfois des lieux ouverts au public, cf. supra sur la France). Pour les autres pays, on est en présence de vidéosurveillances soit admises dans les lieux privés et les lieux publics, tels que l'Italie et le Royaume-Uni, les Pays-Bas[25], le Portugal, soit admises dans les lieux privés, tel que le Danemark (où les vidéosurveillances dans les lieux publics sont cependant admises sous conditions restrictives)

[20] L'examen ne porte pas sur les législations des pays suivants : Danemark et Irlande .
[21] Ce point spécifique n'a pas pu être vérifié pour les pays suivants : Danemark et Irlande.
[22] Loi n° 95-73 du 21 janvier 1995 et décret n° 96-926 du 17 octobre 1996
[23] Loi 1998 :150 relative à la vidéosurveillance générale
[24] Loi 1995 :1506 sur la vidéosurveillance secrète
[25] Les vidéosurveillances privées sont admises, sous des conditions restrictives

Délibération n°89/2005 du 21 décembre 2005 de la Commission nationale pour la protection des données relative à la demande d'autorisation préalable introduite par l'établissement public Domaine Thermal de Mondorf en matière de traitement à des fins de surveillance contenant des données biométriques.

I. Procédure et forme de la demande

L'établissement public de droit luxembourgeois Domaine Thermal de Mondorf (ci-après désigné « le requérant »), établi et ayant son siège à L-5601 Mondorf-les-Bains, Avenue des Bains, a introduit par requête du 31 octobre 2005, une demande d'autorisation, enregistrée sous les références R002245 / A002062, sur base de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après en abrégé « la loi »).

La Commission nationale pour la protection des données (ci-après « la Commission nationale ») constate que le requérant s'est désigné lui-même comme responsable du traitement, en indiquant comme son représentant Monsieur Marc OLINGER, Directeur.

- Compétence

La Commission nationale se déclare compétente pour examiner la demande d'autorisation sur base des articles 3, 10, 14 paragraphe (1) lettre (a), 32 paragraphe (3) lettre (d) et 33 paragraphe (1) lettre (c) de la loi.

- Recevabilité

La demande d'autorisation est recevable, étant donné que celle-ci contient toutes les informations obligatoires mentionnées à l'article 14 paragraphe (2) de la loi.

- Quant aux formalités préalables à l'autorisation de traitement prescrites par la loi

La Commission nationale relève que l'article 14 de la loi exige que les demandes d'autorisation doivent être préalables à la mise en œuvre du traitement envisagé. Son paragraphe (4) prévoit d'ailleurs que, dans le cas contraire, le contrevenant s'expose à des peines correctionnelles.

En l'espèce, le requérant a déposé sa demande d'autorisation le 31 octobre 2005 alors que le traitement a été mis en oeuvre depuis le 21 septembre 2005.

Dans son courrier du 23 septembre 2005, la Commission nationale avait rendu le requérant attentif à ce problème et avait exigé la cessation immédiate du traitement en question jusqu'à ce qu'elle se prononce formellement sur le traitement mis en place.

Il convient de préciser que dès la mise en place du traitement un certain nombre d'abonnés s'étaient plaints auprès de la Commission nationale parce que les agents du Centre thermal menaçaient de leur interdire l'accès aux installations en tant qu'abonnés dès lors qu'ils refuseraient de se prêter à la collecte de leurs empreintes digitales et d'utiliser à l'avenir le système en question lors de leur accès aux installations ; le requérant leur proposait alors le remboursement du solde de l'abonnement.

Dans un courrier du 28 septembre 2005, la Commission nationale informait la direction du Domaine Thermal qu'elle ne saurait accepter que ces personnes subissent un traitement désavantageux au niveau des conditions financières et des modalités pratiques de l'accès aux installations et ce aussi longtemps que la Commission nationale n'aurait pas statué sur la demande d'autorisation. Dans l'attente de prendre position sur le traitement envisagé, la Commission a exigé que le requérant propose des mesures alternatives pour les abonnés qui refusent de donner leurs empreintes digitales. Les responsable du Centre thermal avaient alors répondu que ces personnes pourraient continuer à utiliser leur abonnement sans devoir fournir leurs empreintes digitales, qu'elles seraient conduites à l'accueil par un préposé pour accéder aux installations et qu'elles n'avaient pas non plus à subir un quelconque délai d'attente.

Or, il semblerait qu'aujourd'hui le requérant ne propose plus cette alternative : les abonnés qui refusent de donner leurs empreintes digitales reçoivent des tickets, à l'instar des visiteurs journaliers, de sorte qu'ils subissent les délais d'attente. La Commission nationale regrette que le Centre thermal n'ait pas respecté ses recommandations.

II. Objet de la demande et bien-fondé

- Description du traitement envisagé

Depuis le 21 septembre 2005, le requérant a mis en place un système d'accès à ses installations réservé à ses clients abonnés au service « Le Club » (ci-après, les abonnés).

Il ressort de la lecture des différentes brochures du requérant que les patients qui suivent le programme DBC en 24 ou 12 séances sont assimilés aux abonnés : il faut donc en déduire que ces patients profitent également de l'accès privilégié et doivent se plier à la prise d'empreintes digitales.

Lors de l'enregistrement de son abonnement, la personne concernée doit fournir à l'hôtesse d'accueil un ensemble de données déterminées : elle se fait photographier et remet ses données d'identification (nom, prénom, adresse, téléphone), ses données bancaires et une donnée biométrique, à savoir une image de son empreinte digitale.

La Commission note qu'il ressort des plaintes qu'elle a reçues que les personnes ayant souscrit un abonnement avant le 21 septembre 2005 doivent également remettre leurs données biométriques lors de leur première visite après le 21 septembre 2005.

Pour enregistrer ladite donnée biométrique, le futur abonné doit déposer son doigt sur le capteur d'un appareil du requérant. De préférence, l'abonné doit remettre son index droit, mais l'abonné peut choisir de poser un autre doigt (par exemple à cause d'une mutilation).

Cet appareil capture l'image de l'empreinte. Suivant la demande d'autorisation,, le logiciel contenu dans l'appareil enregistreur extrait uniquement quatre minuties (ce que le requérant appelle dans sa demande les "4 Points de Comparaison"). Une minutie est l'arrangement particulier des lignes papillaires formant des points caractéristiques à l'origine de l'individualité des dessins digitaux (ex. arrêt de lignes, bifurcations, lacs, îlots, points). Le logiciel va ensuite calculer, à partir de ces quatre minuties, une valeur de contrôle grâce à une formule algorithmique ; cette valeur est une suite numérique qui est appelée gabarit ou valeur de référence. L'image de l'empreinte est dès lors transformée en gabarit. Il résulte de la demande que le logiciel va sauvegarder le gabarit et que l'image de l'empreinte digitale est détruite.

Le processus relatif à l'empreinte digitale ci-avant décrit constitue l'enrôlement.

Toutes les données collectées – et notamment le gabarit – sont centralisées dans une base de données unique. Cette base de données enregistrera également les services reçus par l'abonné dans les installations du Centre thermal. Chaque abonné est reconnu par un numéro d'identification unique.

A l'issue de son enregistrement, l'abonné se voit remettre un bracelet-chip sur lequel figure uniquement son numéro d'identification.

L'abonné se présente avec son bracelet-chip devant les bornes qui lui sont réservées près des tourniquets : il présente son bracelet devant la borne.

Cette opération permet de reconnaître la personne dans la base de données : les données de cette personne sont alors « extraites ».

Ensuite, le capteur se trouvant sur la borne va capter l'image de l'empreinte du même doigt que l'abonné a choisi lors de l'enrôlement.

Le logiciel contenu dans la borne va alors scanner l'image digitale et, après avoir appliqué la formule algorithmique choisie pour l'enrôlement, la comparer aux données de l'abonné enregistrées dans la base de données.

Le tourniquet est débloqué si la comparaison des deux empreintes est positive.

Compte tenu de la particularité du traitement envisagé, la Commission nationale a recouru aux services d'un consultant indépendant pour la conseiller dans les questions techniques et de sécurité : une visite des lieux s'est déroulée le 28 novembre 2005 en présence notamment de représentants de la direction du Centre thermal.

Le consultant a examiné les modalités et caractéristiques techniques du système et remis un rapport détaillé à la Commission nationale dans lequel il a relevé notamment qu'il ne peut pas exclure sans laisser des doutes qu'outre les minuties, l'empreinte digitale intégrale soit stockée dans la base de données. La documentation technique et exhaustive communiquée par le requérant précise qu'à chaque passage sur le capteur l'image de l'empreinte digitale est enregistrée. Si l'image scannée à la borne est plus nette et précise que le gabarit celui-ci est effacé et l'image nouvellement scannée va alors servir de référence pour les comparaisons ultérieures.

A l'expiration de la validité de son abonnement, toutes les données à caractère personnel de l'abonné sont supprimées de la base de données.

1. A titre préliminaire : l'applicabilité de la loi

Les traitements contenant des données biométriques ne sont pas expressément prévus par la loi du 2 août 2002. Par conséquent, il y a lieu de vérifier, à titre préliminaire, si ladite loi a vocation à s'appliquer.

a) Donnée biométrique et donnée à caractère personnel

Il se pose la question de savoir si une donnée biométrique répond à la définition de données à caractère personnel donnée par la loi du 2 août 2002.

La biométrie est « l'exploitation automatisée de caractéristiques physiologiques ou comportementales pour déterminer ou vérifier l'identité » (IBG, International Biometric Group).

La biométrie est donc la transformation des caractéristiques physiques d'un individu en une suite numérique.

Il a été précisé que les systèmes biométriques sont « des applications permettant l'identification automatique ou l'éligibilité d'une personne à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main, etc.), de traces (ADN, sang, odeurs), ou d'éléments comportementaux (signature, démarche) » (CNIL, 22e rapport d'activité 2001, « un siècle de biométrie »).

Une donnée biométrique est donc une caractéristique physique d'un individu qui est traduite en une suite informatique et numérique.

L'article 2, lettre (e), de la loi définit la donnée à caractère personnel comme « toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable (" personne concernée") ; une personne physique ou morale est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ».

La Commission Nationale de l'Informatique et des Libertés (ci-après : CNIL) a estimé que « par nature, un élément d'identification biométrique ou sa traduction informatique sous forme de gabarit constitue une donnée à caractère personnel entrant dans le champ d'application des lois « informatique et libertés » comme d'autres données personnelles (un nom, une adresse, un numéro de téléphone, etc.). La finalité de ces techniques consiste en effet, pour l'essentiel, à reconnaître une personne physique, à l'identifier, à l'authentifier, à la repérer » (CNIL, 22e rapport d'activité 2001, p.166).

Le Tribunal de Grande Instance de Paris suit cette définition : dans un jugement du 19 avril 2005 (CE Effe Services, Syndicat Sud Rail c/ Effia Services), il a ainsi décidé qu'une « empreinte digitale, même partielle, constitue une donnée biométrique morphologique permettant d'identifier les traits spécifiques qui sont uniques et permanents pour chaque individu ».

En l'espèce, le gabarit de l'empreinte digitale figure dans la base de données centralisée.

Par conséquent, et au vu des développements ci-avant exposés, l'image d'une empreinte digitale et le gabarit sont des données à caractère personnel telles que définies par la loi du 2 août 2002.

b) Le traitement de données au sens de la loi et le traitement de données biométriques

Il convient de déterminer si un traitement contenant une ou plusieurs donnée(s) biométrique(s) est un traitement au sens de la loi.

L'article 2, lettre (s) de la loi donne une définition précise de la notion de traitement de données à caractère personnel.

En France, la CNIL a retenu que « lorsque le traitement des données biométriques suppose la conservation et le stockage des gabarits, il y a constitution d'une base de données qui relève alors de l'ensemble des dispositions des lois de protection des données au premier rang desquelles figurent le principe cardinal de la finalité et le principe implicite de nos législations qui en est le corollaire : le principe de proportionnalité » (CNIL, 22e rapport, p.167). Il échet de préciser que la définition de traitement qui figure dans la loi du 2 août 2002 est identique à celle donnée à l'article 2, paragraphe (3) de la loi française coordonnée n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La solution donnée par la CNIL est transposable à notre législation.

Dès lors, le traitement de données biométriques envisagé par le requérant est à qualifier de traitement de données à caractère personnel et la loi du 2 août 2002 a vocation à s'appliquer.

c) La qualification du traitement envisagé par le requérant

L'article 2, lettre (q), de la loi définit la surveillance comme « toute activité faisant appel à des moyens techniques en vue de détecter, d'observer, de copier ou d'enregistrer des mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile ».

Il ressort des travaux parlementaires que « le projet de loi [n°4735] inclut les traitements de données à des fins de surveillance comme par exemple la vidéosurveillance ainsi que toute forme de surveillance électronique » (n°4735/0 p.36 et 4735/13 p.97).

La doctrine a retenu que la surveillance des mouvements vise « tous les dispositifs permettant de détecter les mouvements des personnes. Outre les caméras, tombent dans cette catégorie des détecteurs de mouvements, à condition toutefois qu'ils permettent d'identifier, directement ou non, une personne. Sont surtout visés ici les (…) portiques et points de passage qui identifient les personnes qui les franchissent » (La Protection des données personnelles, Cyril Pierre-Beausse, éd. Promoculture, n°162).

En l'espèce, le système décrit dans la demande d'autorisation, utilise une borne d'accès qui détecte et enregistre les mouvements des personnes (abonnés, curistes DBC) saisies dans le fichier afférent voulant accéder aux installations du « Club ».

Par conséquent, il s'agit d'un traitement à des fins de surveillance : le traitement envisagé tombe dans le champ d'application de l'article 10 de la loi.

2. Finalité et légitimité du traitement envisagé

a) Finalité

Les finalités du traitement envisagé sont décrites dans la demande d'autorisation de la manière suivante :

« (i) le contrôle de l'accès au Site et la lutte contre la fraude et

(ii) une gestion commerciale optimisée du Site, pour le décompte des entrées sur le compte des Abonnés »

Aux termes de l'article 4 paragraphe (1) lettre (a) de la loi, le responsable du traitement doit s'assurer que les données sont « collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ».

Il est vrai que la fraude peut avoir des conséquences préjudiciables, voire ébranler la pérennité économique d'une exploitation. En effet, d'une part, l'exploitant est contraint de répercuter le coût que représente pour lui la fraude sur les personnes qui profitent licitement de son installation : le prix des prestations est ainsi majoré pour compenser les pertes financières causées directement par la fraude. D'autre part, la tolérance de la fraude donne une mauvaise image du professionnel : plus la fraude est facile, plus elle incite également les contrevenants à revenir et cela ouvre des perspectives à des personnes mal intentionnées qui voudraient profiter illicitement des installations. Dès lors, la volonté d'éliminer les risques de fraude rassure également les personnes qui ne fraudent pas et qui payent leurs prestations sans poser de difficultés.

Le requérant a donc un intérêt économique évident à profiter de l'évolution technologique pour combattre la fraude et optimiser le fonctionnement de son entreprise.

Les impératifs légitimes qu'il avance sur le plan de la gestion commerciale comprend tant la recherche du confort des abonnés qui se rendent dans les installations que la réduction des coûts économiques liés à la diminution du personnel qui contrôlaient physiquement les flux des personnes entrant dans le site, et plus particulièrement, le flux des abonnés.

Au vu de ce qui précède, la Commission nationale considère que les finalités décrites dans la demande d'autorisation sont déterminées, explicites et légitimes au sens de l'article 4 paragraphe (1) lettre (a) de la loi.

Elle rappelle toutefois que, conformément à l'article 4 de la loi précitée, l'utilisation des données traitées doit se limiter aux finalités pour lesquelles elles ont été collectées.

b) Légitimité

La Commission nationale note qu'un traitement à des fins de surveillance (que ce soit le régime général visé à l'article 10 ou le régime particulier prévu à l'article 11) doit, pour être licite, être effectué conformément aux dispositions de l'article 4 de la loi (cf. document parlementaire 4735/13, p. 17).

Dérogeant à l'article 5 qui traite des conditions de légitimité générales, l'article 10 de la loi détermine les hypothèses dans lesquelles une surveillance peut être effectuée, lesquelles sont au nombre de trois (cf. document parlementaire 4735/13, p. 17). Les cas d'ouverture permettant cette surveillance sont limitatifs (cf. document parlementaire 4735/00, p. 98).

En l'espèce, la demande d'autorisation est basée sur l'article 10, paragraphe (1), lettre (a) de la loi parce « que les personnes concernées donnent leur consentement à la collecte et au traitement des Données, et en particulier des Points de Comparaison ».

La notion de consentement figurant à l'article 2, lettre (c), de la loi est plus rigoureuse que celle donnée par la directive 95/46/CE : la loi définit en effet le consentement comme « toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée (…) accepte que les données à caractère personnel fassent l'objet d'un traitement. »

Dans sa demande, le requérant précise que le consentement, « recueilli lors de la souscription à un abonnement » est « (a) informé, au moyen de la brochure [explicative] ; (b) spécifique, car les conditions générales ne sont applicables qu'à l'accès au Site et les Points de Comparaison sont exclusivement utilisés en vue de la Vérification ; et (c) libre, car celle-ci peuvent choisir un mode d'accès au Site autre que l'abonnement, et ainsi ne pas être soumis à la Vérification. »

Il convient d'analyser si les éléments constitutifs du consentement tels que définis à l'article 2, lettre (c) de la loi sont effectivement réunies en l'espèce :

- Un consentement exprès et non équivoque

« Le consentement de la personne au traitement de ses données doit être exprès et non équivoque. Aucune forme écrite et aucune formule sacramentelle ne sont requises. » (cf. Doc. Parl. 4735/13).

Il en résulte qu'un consentement implicite ou tacite ne répond pas aux exigences de la loi et n'est dès lors pas suffisant pour légitimer un traitement de données.

Il résulte de la demande que le préposé du requérant recueille directement le consentement exprès et non équivoque des abonnés.

La Commission nationale estime donc que le consentement des abonnés est exprès et non équivoque.

- Un consentement libre

Le Code civil ne définit pas la notion de consentement.

La doctrine retient que le terme consentement désigne « la manifestation de volonté de chacune des parties, l'acquiescement qu'elle donne aux conditions du contrat projeté. C'est avec cette signification que le mot consentement est employé lorsqu'on parle de « l'échange de consentements » ou encore lorsqu'on dit d'une personne qu'elle « a donné consentement » (Les obligations, Précis Dalloz, extrait n°85).

Il ressort des travaux parlementaires que les articles 1112 et suivants du Code civil doivent servir de lignes directrices pour apprécier le caractère libre du consentement (cf. doc. parl. 4735/13, p.5).

L'article 1112, alinéa 1er, du Code civil dispose qu'il « y a violence lorsqu'elle est de nature à faire impression sur une personne raisonnable, et qu'elle peut lui inspirer la crainte d'exposer sa personne ou sa fortune à un mal considérable et présent ».

La jurisprudence luxembourgeoise retient qu'il « n'y a violence que lorsque celle-ci atteint un degré de gravité suffisant et qu'il existe un danger raisonnable pour la personne ou les biens du contractant » (Tribunal d'arrondissement de Luxembourg, 7 avril 1948, 14, 399).

Il faut en conclure que la notion de violence – et donc l'absence de consentement libre – est entendue de façon très restrictive.

Or, la théorie générale dégagée en droit civil n'est pas transposable à la matière spécifique de la protection des données pour apprécier si un consentement est libre.

En effet, les travaux parlementaires précisent encore que « la liberté du consentement doit s'apprécier au cas par cas au regard des circonstances de l'espèce » et, comme il a déjà été dit, que les articles 1112 et suivants du Code civil doivent servir de lignes directrices en la matière.

La doctrine retient en effet qu'en matière de protection des données, la contrainte « peut découler de la situation juridique ou économique dans laquelle est placée la personne concernée, par rapport au responsable du traitement » (La Protection des Données Personnelles, Cyril Pierre-Beausse, Promoculture 2005, extrait 74).

Ainsi, «dans une situation économique qui met en relation une personne faible (la personne concernée) et une personne dominante (le responsable du traitement), comme, par exemple, lors de l'obligation de contracter un prêt bancaire ou une assurance-vie, peut-il s'avérer fort probable que le consentement de la personne concernée n'est pas forcément libre, alors qu'il lui est demandé de fournir telle ou telle donnée à caractère personnel « nécessaire » pour que la conclusion du contrat qui entraînera la prestation de service nécessitée puisse avoir lieu. De ce fait, le consentement de la personne concernée est une condition primordiale de licéité d'un traitement de données à caractère personnel. » (doc. parl. 4735/0, p.27).

La contrainte (sous laquelle le consentement peut être recueilli) peut donc résulter de la situation juridique ou économique dans laquelle se trouve la personne concernée par rapport au responsable du traitement.

La doctrine retient que « l'utilisation de la biométrie doit demeurer volontaire. Le consentement doit être libre, spécifique et informé. Cela suppose que le consommateur (la personne concernée) ait à disposition d'autres alternatives s'il ne souhaite pas que des données biométriques le concernant soient collectées et traitées. (…) Le consentement sera en particulier libre si elle [la personne concernée] n'éprouve pas de réticence par rapport à l'utilisation des données biométriques la concernant. Lorsqu'il n'est pas possible d'obtenir un consentement libre, notamment lorsque la personne concernée se trouve dans une situation de subordination ou dans un rapport déséquilibré qui ne lui laisse pas de véritable choix, (…) le recours à la biométrie ne peut intervenir que si la loi le prévoit… » (Quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé, Jean-Philippe Walter, 26e Conférence internationale des Commissaires à la protection des données et à la vie privée, septembre 2004, p.8).

Pour que le consentement soit libre, encore faut-il que le requérant offre des alternatives aux personnes qui refusent le traitement de leurs données biométriques.

En l'espèce, les abonnés qui refusent de remettre leurs données biométriques ont la possibilité d'accéder aux installations mais uniquement en payant plus cher le service (par exemple une entrée journalière ou un carnet à entrées multiples). La possibilité de prendre un abonnement sans devoir se soumettre à la prise d'empreintes digitales n'est pas offerte.

Il convient de remarquer en outre que le requérant a une position unique au Luxembourg. Le requérant est un établissement public, certes à caractère industriel et commercial, qui, financièrement, doit tenir en équilibre son exploitation, mais qui en même temps exerce une mission d'intérêt public. Le requérant occupe sur le marché du Grand-Duché de Luxembourg une place que l'on peut considérer comme unique, entre autres de par sa taille et la diversité de ses services. Il s'agit par ailleurs du seul établissement « thermal » au Grand-Duché » et il n'existe pas d'autres établissements comparables à celui du requérant. Les curistes doivent, obligatoirement venir suivre leur programme chez le requérant. Dès lors, on peut considérer que le requérant est en position quasi monopolistique au Grand-Duché, alors qu'il n'existe pas de concurrent potentiel offrant des prestations tout à fait identiques.

Le consentement des patients suivant le traitement médical DBC pourrait être contraint alors qu'ils ont d'abord choisi de suivre un programme médical – programme que le requérant est le seul à le proposer au Grand-Duché -, et que ce programme sous-entend la condition d'abonné : se trouvant devant un fait accompli ils n'ont pas d'autre choix que celui d'être soumis à un traitement de données biométriques.

Compte tenu de ces éléments, la Commission nationale s'interroge sur le point de savoir si le consentement des personnes concernées peut dans tous les cas être considéré comme étant donné de façon absolument libre.

- Un consentement spécifique et informé

« Le consentement doit être spécifique, en ce qu'il ne peut porter que sur des traitements déterminés. C'est dans cette optique que le responsable du traitement doit informer la personne concernée sur la ou les finalités déterminées du traitement auquel les données sont destinées. Si plusieurs finalités sont poursuivies par un même traitement, le responsable du traitement doit en informer la personne concernée. » (cf. Doc. Parl. 4735/13).

Le droit à l'information est une notion essentielle de la loi.

« La personne concernée doit [en effet] donner son consentement en connaissance de cause, ce qui explique une nouvelle fois le lien entre le consentement de la personne concernée avec le principe de la qualité des données prévu à l'article 4, paragraphe (1) lettre (a), et avec le droit à l'information prévu à l'article 26. Ce droit à l'information doit s'exercer soit lors de la collecte des données auprès de la personne concernée, soit lors de l'enregistrement ou la première communication à un tiers pour les données qui n'ont pas été collectées auprès de la personne concernée. » (cf. Doc. Parl. 4735/13).

En vertu de l'article 10, paragraphe (2) et l'article 26 de la loi, le responsable du traitement doit informer les personnes concernées de la mise en œuvre de la surveillance.

Le droit à l'information implique que la personne concernée soit informée de ce qui suit :

« (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 la concernant et de rectification de ces données ;
- la durée de conservation des données ».

De plus, il convient d'apprécier in concreto la liste des informations supplémentaires telles que prévues à la lettre (c). Ainsi, « le responsable du traitement devra fournir toutes les informations supplémentaires nécessaires compte tenu des circonstances particulières dans lesquelles les données sont collectées, pour assurer à l'égard de la personne concernée un traitement loyal des données, c'est-à-dire une information pleine et entière. La liste de ces informations supplémentaires n'est pas exhaustive. » (travaux parlementaires, 4735/13, page 24).

La Commission estime que, compte tenu de la nature sensible des données biométriques, l'information doit également porter sur l'existence et la catégorie de destinataires à qui les données sont communiquées ainsi que sur la durée de conservation et sur l'existence du droit d'accès et sur le fait que les données sont centralisées. Le requérant doit également informer les personnes concernées sur le fait qu'à chaque passage à la borne, leur empreinte digitale est enregistrée et que si elle est plus précise que celle qui figure dans la base de données, alors la nouvelle image sera sauvegardée et sera utilisée pour les comparaisons ultérieures.

En outre, « le principe d'un traitement loyal des données à caractère personnel suppose que la personne concernée soit informée des aspects du traitement qui sont pertinents pour elle. Les propriétés du système qui reposent de façon inhérente sur des probabilités et donc sont faillibles, constituent un tel aspect pertinent. Aussi, il revient au responsable du traitement d'informer la personne concernée sur ce fait et sur ce qu'elle peut faire si elle est victime de ce système. Toute présomption d'infaillibilité est erronée » (Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, février 2005, Conseil de l'Europe, extrait n°31).

En effet, le résultat d'une comparaison est toujours une estimation. La personne concernée doit dès lors être informée lors de la collecte qu'il existe un pourcentage d'échec de reconnaissance de son gabarit. Dès lors, la Commission nationale considère que le requérant doit avertir les personnes concernées de la possibilité que leur donnée biométrique ne soit pas reconnue lors de l'opération de comparaison des gabarits.

Le droit à l'information est une obligation de résultat, de sorte qu'en cas de contestation, le requérant devra rapporter la preuve que la personne concernée a été informée (travaux parlementaires, 4735/13, page 24).

« Bien souvent, la crainte qu'une parfaite information ne conduise les personnes à refuser de consentir ou une certaine approche commerciale du problème peuvent contribuer à dégrader l'exigence du consentement » (Acadaméie des Sciences Morales et Politiques, « Société d'information et vie privée », Tome 3, Chapitre 1, « La protection des données personnelles à la croisée des chemins », édition Presses Universitaires de France, Michel GENTOT).

La demande d'autorisation précise que :

« Le consentement est recueilli lors de la souscription à un abonnement. A ce titre, chaque personne concernée se voit remettre une brochure explicative sur les conditions de fonctionnement du Système. (…) ».

De plus, le requérant expose ce qui suit dans sa lettre d'accompagnement à la demande d'autorisation du 31 octobre 2005 :

« [le requérant] est déterminé à mettre en place et à diffuser systématiquement des supports d'information clairs et complets sur le Système, ainsi qu'à répondre promptement à toute demande d'information émanant du public ».

La brochure explicative à laquelle le requérant se réfère précise en effet que les données personnelles et les empreintes digitales seront recensées lors de la première visite. Mais, elle ne donne pas d'information sur les finalités du traitement, sur une communication ou non à des destinataires, sur l'enregistrement des données d'identification, y compris biométriques dans une base de données centrale, sur l'existence d'un taux d'erreur, sur la durée de conservation des données et sur l'exercice du droit d'accès. Le droit à l'information étant une obligation de résultat, il appartient au requérant de démontrer qu'il le respecte.

Le contenu de ladite brochure est insuffisant pour satisfaire aux exigences d'un consentement informé. Par ailleurs, les plaintes et réclamations reçues de la part de certains abonnés laissent entendre qu'aucune information ne leur a été donnée avant la saisie de la donnée biométrique, les abonnés étant simplement invités à déposer leur doigt sur un capteur.

En conclusion, la Commission nationale estime que le requérant ne respecte pas toutes les conditions d'un consentement libre, spécifique et informé des personnes auprès desquelles il recueille des données biométriques qu'il enregistre et traite dans le cadre du système de contrôle des accès, plus amplement décrit ci-avant.

3. Qualités des données

a) Loyauté de la collecte et exactitude des données

Dans sa demande le requérant précise ce qui suit :

« les Données sont recueillies lors de l'abonnement par un préposé du Domaine Thermal et introduites directement dans la Base de Données. Les Points de Comparaison sont collectés au même moment, au moyen d'un dispositif technique spécifique relié au Système »

De plus, selon les informations fournies par le requérant, l'empreinte digitale est collectée successivement à trois reprises afin de limiter le risque d'erreur lors de l'enrôlement des données. Il convient de rappeler que les algorithmes sont conçus pour donner une réponse à la comparaison sous la forme d'un pourcentage de coïncidences. Cette multiplication de l'enregistrement améliore ainsi l'exactitude de la donnée biométrique, même si cela ne permet jamais d'écarter totalement les erreurs de reconnaissance de la donnée biométrique.

En outre, lors de chaque passage, la machine sauvegarde l'image de l'empreinte digitale si elle est plus nette et plus précise que celle qui figure sur sa base de données : cela contribue à l'exactitude des données.

Bien qu'il semble que les personnes concernées ne soient pas spécifiquement rendues attentives à cette procédure, la Commission nationale estime que l'ensemble des données du traitement envisagé est collecté de manière loyale, tel que l'exige l'article 4 de la loi.

b) Le principe de proportionnalité

Selon le principe de proportionnalité, tout traitement des données ainsi que toute mesure prise en relation avec ce traitement, doit être proportionné aux finalités poursuivies. Ce principe implique que le responsable du traitement doit limiter le traitement à des données adéquates, pertinentes et non excessives au regard des finalités à atteindre (cf. article 4 paragraphe (1) lettre (b) de la loi).

- Catégories de personnes concernées

Il ressort de la lecture des différentes brochures que les patients qui suivent le programme DBC en 24 ou 12 séances sont assimilés aux abonnés.

Par conséquent, et bien que la demande d'autorisation ne le mentionne pas expressément, la Commission nationale estime que les personnes concernées par le traitement envisagé sont les personnes ayant souscrit un abonnement au Club et les patients inscrits au programme DBC en 12 ou 24 séances.

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

Le requérant signale que les « données ne sont communiquées à aucun tiers en vue d'un autre traitement (…) Il n'y a pas de destinataires externes ».

Il ressort de ce qui précède qu'il n'y a aucun destinataire externe.

Les seuls destinataires relèvent du personnel du requérant, respectivement des personnes placées sous son autorité et qui agissent pour le compte du requérant, lequel précise dans sa demande ce qui suit :

« Les personnes susceptibles d'accéder aux Points de Comparaison stockés dans la Base de Données sont :

(a) le responsable du service informatique du Domaine Thermal ; et

(b) le gestionnaire des réseaux du Domaine Thermal

(les Destinataires Internes).

De manière incidente, un prestataire de services tiers (le fournisseur du Système) peut également accéder (au moins en théorie) au Système lors d'opérations de maintenance, mais n'est pas à considérer comme destinataire au sens de la Loi. »

Dans le protocole du 20 septembre 2005, il est précisé que « le droit d'accès au logiciel et à la base de données y relative est limitée aux personnes autorisées. Le droit d'accès et le type d'accès dépendent du niveau d'utilisateur défini pour chacun des utilisateurs.

⇨Gestion administrateur du logiciel

- Responsable Mondorf Le Club
- Secrétaire Responsable Mondorf Le Club (gestion club)
- Responsable service informatique
- Gestionnaire des réseaux
- Remplaçant du gestionnaire des réseaux
- Société EWV fournisseur du logiciel

⇨Gestion comptable : Consultation et édition des états financiers

- Caissier principal
- Caissier remplaçant

⇨Gestion clientèle (réception du club et points de vente)

- Hôtesse d'accueil »

Il ressort par ailleurs de la demande qu'en « aucun cas les données recueillies ne font l'objet d'un transfert en dehors de l'Union européenne.»

Les destinataires mentionnés apparaissent aux yeux de la Commission nationale comme étant légitimes, nécessaires et proportionnés au regard des finalités poursuivies.

- Durée de conservation des données

Conformément à l'article 4, paragraphe (1) lettre (d) de la loi, les données traitées ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

Une durée limitée de conservation de données constitue une garantie supplémentaire pour éviter d'éventuels détournements de finalités.

Dans sa demande, le requérant précise ce qui suit :

« Les Points de comparaison sont conservés pendant la durée de l'abonnement et sont ensuite systématiquement détruits ».

Compte tenu du fait qu'à chaque passage à la borne, le logiciel enregistre l'image de l'empreinte digitale et la conserve si elle est plus nette et précise que celle qui figurait préalablement dans la base de données, la Commission nationale tire la conclusion que la donnée biométrique est effacée si, lors d'une comparaison, l'image nouvelle est plus nette. En toute hypothèse et au plus tard, la donnée biométrique est effacée à la fin de l'abonnement.

Par conséquent, la Commission nationale estime que la durée de conservation n'est pas excessive.

- Proportionnalité d'un traitement contenant des données biométriques

Dans le cas spécifique des traitements de données biométriques, il est retenu que « la biométrie, à l'instar de toutes les technologies, est définie par son usage. Les technologies biométriques ne sont, en elles-mêmes, ni nécessairement préjudiciables ni nécessairement favorables à la protection de la vie privée. L'application de ces technologies soulève néanmoins plusieurs problèmes de protection de la vie privée particuliers » (Groupe de travail sur la sécurité de l'information et la vie privée, Technologies fondées sur la biométrie, OCDE, 10 juin 2005, p.13).

En effet, « une mesure biométrique est plus qu'un identifiant numérique [car elle] livre des informations personnelles intimes sur la composition de notre corps et sur notre comportement en général » (Commission d'accès à l'information du Québec, La biométrie au Québec : les enjeux » Document d'analyse, juillet 2002).

Par conséquent, les personnes concernées doivent physiquement se soumettre à chaque passage pour s'identifier. De plus, les données biométriques sont collectées à partir du corps humain.

Il convient de souligner que « l'intégralité du corps humain et la manière dont il est utilisé par la biométrie constituent un aspect de la dignité humaine » (Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, Conseil de l'Europe, février 2005, point n°9).

Le Professeur Roger Clarke de l'Australian National University, estime aussi que le recours à la biométrie présente des dangers particuliers pouvant être regroupés en deux catégories. La première est inhérente aux menaces liées à tous les systèmes informatiques (collecte des données sur les individus, multiplication des informations sur leur comportement, leurs déplacements, les actions…), la seconde "s'attache aux caractéristiques propres à la biométrie : celle-ci donne une information intrinsèquement liée à la personne elle-même (distinction entre "information about the person" et "information of the person") ; la personne doit se soumettre physiquement au processus de vérification. Dès lors, la personne concernée doit coopérer : elle doit physiquement se soumettre à la surveillance.

Du fait de l'intrusion particulière dans la sphère privée, qu'elle implique parfois même une atteinte à la dignité humaine et afin de ne pas banaliser son recours, « la biométrie ne doit pas être utilisée seulement parce qu'elle est pratique, mais parce qu'elle constitue le seul moyen d'atteindre le résultat recherché » (Rapport d'information n°439 du Sénat, session 2004-2005, sur la nouvelle génération de documents d'identité et de la fraude documentaire, p.92).

En d'autres mots, « des données biométriques ne doivent être utilisées que si leur utilisation est adéquate, pertinente et non excessive, ce qui implique une évaluation rigoureuse de la nécessité et de la proportionnalité des données traitées » (Document de travail sur la biométrie, du 1er août 2003, Groupe de travail « Article 29 » sur la protection des données, n°12168/02/FR GT 80, p.8).

Le degré d'intrusion dans la vie privée diffère en fonction du traitement de données biométriques choisi : il existe en effet une diversité de traitements possibles de données biométriques qui sont plus ou moins intrusifs dans la vie privée des personnes concernées.

La Commission nationale doit dès lors vérifier ci-après si le traitement envisagé par le requérant est proportionné par rapport aux buts recherchés. Il convient de rappeler que la Commission a pour mission de contrôler la proportionnalité des traitements soumis à son autorisation. La jurisprudence luxembourgeoise retient à cet effet que « la CNPD doit nécessairement procéder à un contrôle de la proportionnalité des mesures envisagées pour décider si le traitement ainsi préconisé est nécessaire pour assurer les besoins prévus par la loi » (Cour administrative, 12 juillet 2005, rôle 19234 C).

- Catégories de données

  - Les catégories de données décrites par le requérant dans sa demande d'autorisation

A ce sujet, le requérant indique ce qui suit :

« Les catégories de Données qui n'ont pas de rapport direct avec la surveillance (c'est-à-dire, les données nécessaires au traitement commercial) ne sont pas détaillées ici et font l'objet d'une notification séparée. Les seules Données pertinentes dans le contexte de la présente demande sont les Points de Comparaison. (…) ».

Malgré l'affirmation du requérant, les données figurant dans la notification susmentionnée sont nécessaires dans le cadre de la présente demande.

L'accès aux installations n'est possible que si l'empreinte digitale est reconnue dans la base de données comme appartenant à l'individu portant le numéro d'identification figurant sur son bracelet.

Il n'y a donc qu'un seul traitement qui comprend la donnée biométrique et les données décrites dans la notification. D'ailleurs le requérant se réfère à la donnée biométrique dans sa notification.

Afin de se prononcer en pleine connaissance de cause, la Commission nationale considère que les données concernant le traitement envisagé sont toutes les données figurant dans la notification (données d'identification, données financières, photographie et donnée biométrique) et le numéro d'identification.

  - La spécificité de l'empreinte digitale comme donnée biométrique

La CNIL a retenu que « l'empreinte digitale est presque aussi redoutable que les traces ADN car elle est omniprésente : où que l'on aille, il est impossible de ne pas laisser de traces de sa présence ».

A « la différence d'autres données biométriques, [les empreintes digitales] laissent des traces qui peuvent être exploitées pour l'identification des personnes et que dès lors toute base de données d'empreintes digitales est susceptible d'être utilisée à des fins étrangères à sa finalité première » (CNIL, 21e Rapport d'activité, 2000, p.102).

Le risque de dérive est potentiellement plus élevé quand les données biométriques laissent des traces parce qu'elles peuvent « être exploitées à des fins d'identification des personnes à partir des objets les plus divers que l'on a pu toucher ou eu en main (…) » (Rapport de la CNIL du 9 décembre 2003 relatif à la demande d'avis 859.794, p.5).

Il convient de rappeler que toutes les données biométriques ne laissent pas de traces (par exemple, le contour de la main, l'iris, la rétine). Ces données ne présentent pas les mêmes dangers que les données qui laissent des traces : « une base de données de reconnaissance de la voix, de gabarit d'iris, de rétine ou du contour de la main ne peut en aucun cas être utilisée à d'autres fins que de la reconnaissance et d'authentification des personnes qui se présentent devant le capteur » (CNIL, 22e rapport d'activité 2001, p.168). Dans ce cas, le risque de dérive et de détournement de finalité est, dès lors, sans intérêt.

Par conséquent, et en raison du risque très limité de l'exploitation ultérieure de données biométriques qui ne laissent pas de traces, les traitements incluant de telles données ne laissant pas de traces sont facilement acceptables.

Ainsi, en Grèce, l'«Authority for the Protection of Personal Data » (APPA) a précisé dans sa décision n°9/2003 du 31 mars 2003 qu'elle encourage les traitements qui ne laissent pas de traces (« Operational recommandations encourage taking advantage of " mild" biometric technologies based on characteristics that do not leave any traces »).

La Commission nationale est a priori plus favorable à autoriser, au stade actuel des technologies utilisées, les traitements de données biométriques qui ne laissent pas de traces compte tenu des risques moindres d'atteinte à la sécurité des données et de détournement de finalité. Ces traitements sont en outre ressentis par les personnes concernées comme bien moins intrusifs dans leur vie privée.

La Commission ne partage pas le raisonnement du requérant quand il prétend que « la collecte des seuls Points de Comparaison place le Domaine Thermal (ou les tiers qui, par impossible, pourraient accéder de manière non autorisée au Système et/ou à la base de Données, ou encore au contenu de la Carte en cas de perte ou de vol de celle-ci) dans l'impossibilité de reproduire l'Empreinte ni de l'utiliser à d'autres fins que la vérification effectuée lorsque l'Abonné sollicite l'accès au Site. Le risque de divulgation de données biométriques relatives aux Abonnés est donc inexistant ».

Il est vrai que « la transformation d'une empreinte digitale en gabarit est irréversible, il n'y a aucun risque de reconstitution d'empreinte à partir d'un gabarit » (8e rapport d'activité du Préposé fédéral à la protection des données en Suisse).

Mais une empreinte digitale est très facile à extraire (par exemple sur un verre) : il existe donc un risque qu'une empreinte soit collectée et d'y appliquer un algorithme précis pour voir si le gabarit est reconnu dans la base de données qui utilise cet algorithme, et ainsi obtenir les données à caractère personnel de cette personne.

De plus, lors de la visite sur les lieux, le requérant n'a pas donné la certitude que l'image non cryptée de l'empreinte n'était pas sauvegardée dans la base de données. Le consultant indépendant affirme ainsi qu'il « ne peut pas être exclu que des informations suffisantes pour reproduire une empreinte ne sont pas enregistrées dans le système. La quantité de données sauvegardées du « fused image » n'est pas indiquée dans la documentation ».

Par conséquent, la transformation de l'image de l'empreinte digitale en gabarit n'exclut pas l'utilisation des données à caractère personnel à des fins détournées.

- La proportionnalité en termes d'opérations de traitement : la centralisation des données biométriques

Dans sa demande, le requérant a indiqué que le traitement envisagé avait deux finalités, à savoir, d'une part, le contrôle de l'accès au site et la lutte contre la fraude (c'est-à-dire que le titulaire du bracelet-chip est bien la personne qui se présente aux installations) et, d'autre part, la gestion commerciale du site relative au décompte des entrées des abonnés.

La Commission nationale reconnaît que le requérant doit pouvoir apprécier le traitement qu'il estime le plus approprié pour parer à la fraude, pour optimiser le fonctionnement de l'établissement et gérer commercialement son site, deux finalités qui sont tout à fait légitimes pour un acteur économique de son envergure.

Mais les moyens adoptés par le requérant pour atteindre ces finalités doivent être les plus respectueux possible des droits fondamentaux et des libertés de la personne concernée : or, tout système centralisé de données – comme le traitement envisagé par le requérant - présente un risque particulier de dérive, qui n'existe pas quand les données ne sont pas centralisées.

Qui plus est, les systèmes de centralisation de données biométriques qui laissent des traces, comme les empreintes digitales, présentent plus de risques pour la protection des libertés et des droits fondamentaux de la personne que les traitements qui ne prévoient pas une telle centralisation.

Ce n'est pas parce qu'un traitement contient des données biométriques que les dangers sont écartés.

Ainsi, les données biométriques « ont la réputation d'être extrêmement fiables car elles paraissent liées à la présence physique et réelle d'une personne et, à ce titre, seraient donc inaliénables. Il existe réellement une forte probabilité que l'usage des données biométriques permette d'être assuré d'avoir affaire à la bonne personne. Néanmoins, les falsifications sont toujours possibles. Les empreintes digitales relevées sur un verre peuvent par exemple servir à créer avec de la cire une empreinte analogue sur un support de stockage » (Rapport d'étape, pré. cit. p.12).

La Deutsche Bank a réalisé une étude (Deutsche Bank Research « Biométrie, mythe et réalité », 22 mai 2002) qui met en exergue les défauts des systèmes biométriques. Ces derniers sont soumis aux mêmes types d'attaques ou de manipulations. Un « hacker » peut ainsi intercepter le gabarit de référence ou le gabarit présenté lors de la phase de comparaison. Néanmoins les conséquences ne sont pas les mêmes car, si un nouveau mot de passe ou un nouveau code peuvent être attribués, la caractéristique biométrique ne peut être modifiée.

Dès lors, le recours à un traitement de données biométriques n'écarte pas le risque de réutilisation des données centralisées. Mais les conséquences peuvent être particulièrement dommageables lorsqu'il s'agit de données biométriques qui laissent des traces.

Les données biométriques qui laissent des traces permettent en effet de remonter à une personne déterminée.

Comme pour tout traitement de données, « la conservation dans un traitement des empreintes digitales est susceptible d'être utilisée à des fins étrangères à la finalité que son concepteur lui avait initialement assignée. En effet, et à la différence d'autres données biométriques (…) les empreintes digitales laissent des traces de chacun de nos gestes les plus quotidiens et peuvent être exploitées à des fins d'identification et de recherche des personnes. Dès lors, une base de données d'empreintes digitales, quelle que soit la finalité initiale de sa constitution, est susceptible d'être utilisée à des fins de police. (…) Quoiqu'il en soit, la connotation policière ne résulte pas uniquement de ce que la prise d'une empreinte digitale est, à l'origine, une technique policière. Elle est bien plus généralement liée à ce que dans la plupart des cas, si ce n'est pas tous, la constitution d'un fichier d'empreintes digitales, même à des fins qui ne sont pas illégitimes, va devenir un nouvel instrument de police, c'est-à-dire un outil de comparaison qui pourra être utilisé à des fins policières, nonobstant sa finalité initiale. Il pourrait presque être soutenu que l'empreinte digitale est (…) une information particulière qui présente un risque réel de relâchement du principe de finalité des fichiers » (Rapport d'ensemble relatif à diverses applications de contrôle d'accès utilisant un dispositif de reconnaissance des empreintes digitales, CNIL, 20 octobre 2000, p.2 et 6).

Il a encore été précisé qu'une « société qui favoriserait le développement de bases de données d'empreintes digitales par exemple, offrirait des moyens considérables et nouveaux - au moins dans l'ordre des « possibles » - d'investigations policières sans forcément qu'un tel objectif ait été initialement recherché. Non pas que les bases de données ainsi constituées l'auraient été à des fins policières mais parce que de telles bases de données, apparemment tout à fait anodines, pourraient être utilisées par la police comme élément de comparaison et de recherche dans le cadre de ses investigations » (CNIL, 22e rapport d'activité 2001, p.108).

Il faut éviter autant que possible tout risque de réutilisation des données biométriques qui permettent de retrouver facilement un individu en particulier.

Ainsi, la CNIL accepte les traitements de données biométriques ayant pour but la vérification des personnes uniquement lorsque le gabarit d'une empreinte digitale est stocké sur un support individuel exclusivement détenu par la personne concernée et dont celle-ci décide librement de l'utilisation (par exemple, délibérations n°03-015 du 24 avril 2003 et n°2005-115 du 7 juin 2005).

Le Groupe de travail « Article 29 » sur la protection des données a pris position sur les deux systèmes : il est « d'avis que l'utilisation, à des fins de contrôle d'accès (…), de systèmes biométriques se référant à des caractéristiques qui ne laissent pas de traces (par exemple la forme de la main, mais non les empreintes digitales) ou de systèmes biométriques se référant à des caractéristiques physiques qui laissent des traces, mais dont les données ne sont pas enregistrées dans une mémoire détenue par une personne autre que la personne concernée (autrement dit, les données ne sont pas mises en mémoire dans le dispositif de contrôle d'accès ou dans une base de données centrale), crée moins de risques pour la protection des libertés et des droits fondamentaux de la personne » (Document de travail sur la biométrie adopté le 1er août 2003, n°12168/02/FR, p.7).

En Allemagne, le « Landesbeauftragte für den Datenschutz Niedersachsen » a écrit dans son rapport n°17 pour l'année 2003-2004 ce qui suit :

« Datenschutzprobleme entfallen weitgehend, wenn auf eine zentrale Speicherung verzichtet wird und die Betroffenen das Speichermedium, zum Beispiel eine Chipkarte, selbst verwalten. »

De plus, Monsieur Peter SCHAAR, „Bundesbeauftragte für den Datenschutz", dans le cadre du colloque „Adlershofer Kolloquium" du 28 juin 2005 recommande notamment que „dass nach Möglichkeit auf eine zentrale Speicherung der Daten verzichtet wird, z. B., durch Speicherung der Daten auf einer Chipkarte oder einem Ausweis".

Dans le même sens, le Dr. G. Laßmann écrit ce qui suit :

„Werden die biometrischen (Referenz-)Daten beim Nutzer (z.B. auf einer Chipkarte, einem Token oder einer anderen mobilen Speichereinheit) gespeichert, so hat dieser eher die Möglichkeit der Kontrolle über seine Daten. Ein zentraler Datenbestand birgt dagegen Gefahren für das informationelle Selbstbestimmungsrecht, nicht zuletzt wegen der weitgehenden Übermittlungsbefugnisse im Privatbereich und der umfassenden Datenerhebungsbefugnisse der Strafverfolgungsbehörden. Je mehr Daten zentral abgelegt werden und auf diese zumindest theoretisch zugegriffen werden kann, je größer sind die Begehrlichkeiten, die bei Behörden und privaten Stellen entstehen können. ..... Ein weiteres Problem besteht darin, dass zentrale Datenbestände üblicherweise ohne Wissen (und Zutun) des Benutzers ausgewertet werden können, was ebenso dessen Selbstbestimmungsrecht einschränkt. Der Einsatz identischer Verfahren in unterschiedlichen Anwendungen führt für den Nutzer zu erhöhten Risiken, da sein biometrisches Merkmal als ein (im Gegensatz zu Namen und Adresse) unveränderbares Personenkennzeichen verwendet werden und sein jeweiliges Nutzungsverhalten zu einem umfassenden Profil zusammengeführt werden kann.

Eine dezentrale Speicherung ist daher in den allermeisten Fällen vorzuziehen." (Dr. G. Laßmann, dans „Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren-Kriterienkatalog", TeleTrusT Deutschland e.V., 10 juillet 2002).

En France, la CNIL ne pose pas non plus le principe du refus de collecte de toute donnée biométrique. Elle ne voit pas d'objection par exemple à ce qu'une base de données contienne les gabarits de données biométriques ne laissant pas de traces tels le contour de la main (par exemple, délibération 2005-064 du 20 avril 2005).

Par contre, elle s'oppose avec véhémence au traitement centralisé de gabarits d'empreintes digitales si un tel traitement n'est pas justifié par des impératifs sécuritaires des locaux à protéger (délibération 04-018 du 8 avril 2004 pour un exemple de décision de refus et 04-017 pour un exemple d'avis favorable). La CNIL a ainsi accepté un tel traitement pour la Cogema, la Banque de France, les Aéroports de Paris pour l'entrée dans des zones de haute protection (pour une étude comparative, voir le 22e rapport d'activité 2001, p.170 et la 3e partie du Rapport sur les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre, annexe 4).

Il est intéressant de citer le cas de la demande d'avis n°859.794 formulée par la mairie de Levallois-Perret et la position arrêtée par la CNIL. Cette mairie avait mis en place un traitement destiné à contrôler l'accès à son « roller-parc » au moyen de la reconnaissance d'une empreinte digitale. Le traitement en question reposait sur l'identification des personnes qui voulaient se rendre dans le « roller-parc ». La mairie justifiait ce traitement en arguant qu'elle souhaitait avoir un système qui évitait une gestion trop lourde pour contrôler l'accès au site et elle entendait également éviter toute manipulation de cartes qui peuvent être perdues ou volées et écarter aussi tout risque de fraude.

Ces finalités sont les mêmes que celles invoquées par le requérant dans sa demande d'autorisation.

Dans son rapport, du 9 décembre 2003, le rapporteur, Monsieur Maurice Benassayag, a proposé un avis défavorable à ce projet compte tenu de l'absence d'impératif de sécurité à protéger. Suivant cette recommandation, la CNIL a, dans sa délibération n°03-065 du 16 décembre 2003, donné un avis défavorable à ce traitement.

Le risque de détournement est proportionnellement plus important que les intérêts à protéger par le traitement. Accepter un tel traitement pour contrôler l'accès à un roller-parc revenait à accepter tous les traitements centralisant des données biométriques qui laissent des traces. Il y aurait alors une multitude de bases de données susceptibles d'être détournées.

Cette position est justifiée parce que les données biométriques qui laissent des traces peuvent être exploitées pour l'identification des personnes et, dès lors, toute base de données d'empreintes digitales est susceptible d'être utilisée à des fins étrangères à sa finalité première.

Dans un jugement du 19 avril 2005, le Tribunal de Grande Instance de Paris (1 ère chambre sociale, CE Effa Services, Syndicat Sud Rail c/ Effa Services) a posé le principe que l'utilisation d'une empreinte digitale qui « met en cause le corps humain et [qui] porte ainsi atteinte aux libertés individuelles peut cependant se justifier lorsqu'elle a une finalité sécuritaire ou protectrice de l'activité exercée dans des locaux identifiés. (…) ». Il a ainsi jugé que « le traitement automatisé de ces données (…) à des fins de gestion et de contrôle du temps de présence des salariés n'est ni adapté ni proportionné au but recherché ».

En Grèce, l'autorité grecque pour la protection des données, « Hellenic Data Protection Authority », refuse également la centralisation des données biométriques sauf si elle se justifie pour des raisons impérieuses de sécurité (par exemple, décisions n°245/9 du 20 mars 2000 et n°9/2003 du 31 mars 2003).

En Italie, l'autorité « Garante per la protezione dei dati personali » a également émis un avis défavorable le 21 juillet 2005 à la centralisation des données biométriques sauf s'il n'existe pas d'autres moyens pour parvenir à la finalité recherchée.

En Suisse, le Préposé fédéral à la protection des données (PFPD) a eu à se prononcer le 6 juin 2005 sur le projet pilote « Secure Chek ». Ce projet a pour but d'améliorer le contrôle de la sécurité des données des passagers et de leurs documents de voyage. Dans le cadre de ce projet, le passager « porteur d'un passeport est authentifié à l'aide de données biométriques (gabarits), ayant été saisies au guichet d'enregistrement après le contrôle du passeport du passager et enregistrées de façon décentralisée sur une carte à puce (smart card) » (Résumé du rapport final du 6 juin 2005). Le PFPD apporte une appréciation positive de l'usage des données biométriques mais précise que « toute modification du projet Secure Check allant dans le sens d'un stockage centralisé des données biométriques ou d'un stockage de données brutes nécessiterait, sous l'angle de la protection des données, une appréciation différenciée, qui n'est pas couverte par le présent rapport ».

Dans son 12ème rapport d'activités 2004/2005, le PFPD recommande de prendre en considération entre autres les principes suivants lors du recours à des données biométriques dans le secteur privé :

« Il faut privilégier … l'utilisation de données biométriques n'impliquant pas le tockage de gabarits dans une base de données gérée par un responsable de traitement autre que la personne concernée. Cette procédure ne soulève en principe pas de problèmes particuliers du point de vue de la protection des données, dès lors que le gabarit est conservé sur un support dont la personne concernée a l'usage exclusif (carte à puce, téléphone mobile, etc.)

- Si une base de données est constituée et gérée par un responsable de traitement autre que la personne concernée, l'élément biométrique retenu peut avoir des conséquences sur les libertés et droits fondamentaux. Tel est en particulier le cas lorsque l'élément biométrique laisse des traces, comme l'empreinte digitale. Le recours à un tel élément doit répondre à un intérêt prépondérant qualifié de sécurité.
- - En l'absence d'un tel intérêt, il convient de recourir à un élément biométrique qui limite le risque d'abus, tel que celui ne laissant pas de trace, comme le contour de la main ».

Conclusion

Le requérant ne justifie pas dans sa demande que l'efficacité de sa gestion commerciale, l'accès à ses installations ainsi que la prévention de la fraude auraient été moins bien assurés par un système moins attentatoire aux droits et libertés des personnes concernées.

Le requérant aurait d'autres possibilités pour parvenir à remplir ses deux finalités sans avoir à s'immiscer autant dans la vie privée des personnes concernées. Si, pour parvenir aux finalités indiquées dans la demande (à savoir l'accès au site et éliminer les risques de fraude ainsi que la gestion commerciale), le requérant souhaite absolument recourir à un traitement de données biométriques, il pouvait envisager des traitements alternatifs moins intrusifs dans la vie privée des personnes concernées.

La Commission ne verrait en principe pas d'objection à ce que les données biométriques permettant l'identification d'un abonné soient stockées exclusivement sur un support individuel, comme par exemple, le bracelet-chip et ce, sans constitution et utilisation d'une base de données biométriques centralisée. Dans ce cas, la personne concernée a la maîtrise sur ses propres données et décide librement de leur utilisation.

La Commission nationale considère que même la centralisation des données biométriques pourrait être admise comme proportionnée aux finalités indiquées, dès lors que l'élément biométrique retenu serait de ceux qui ne laissent pas de traces comme, par exemple, le contour de la main.

La constitution de bases de données nominatives associées à des empreintes digitales et son utilisation, même limitée à la comparaison des empreintes aux seules fins de contrôle d'accès à des locaux ou à des services, comportent un risque d'atteinte aux libertés individuelles dans la mesure où elles sont susceptibles d'être utilisée à des fins étrangères aux finalités initialement poursuivies.

La Commission nationale est d'avis que, compte tenu des risques de dérive importants existant pour les fichiers centralisés de données biométriques laissant des traces, il faut circonscrire le recours à ces traitements : de tels traitements ne peuvent être autorisés que si le requérant justifie de raisons impérieuses de sécurité ou de protection de l'activité exercée dans les locaux à protéger.

Admettre le traitement envisagé par le requérant, alors qu'il s'agit simplement de surveiller l'accès à une aire de loisirs, à défaut d'impératifs de sécurité prépondérants, pourrait contribuer à la désensibilisation du public, « en raison d'une utilisation toujours croissante de ces données, aux conséquences que leur traitement peut avoir sur la vie quotidienne » (Document de travail sur la biométrie, Groupe « Article 29 », p.2). Les personnes se résigneraient à donner leurs empreintes digitales sans vraiment mesurer le danger auquel elles s'exposent en cas de réutilisation ou de détournement des données.

En l'espèce, le requérant ne justifie pas de telles nécessités sécuritaires ou protectrices. D'ailleurs, des traitements moins intrusifs pour la vie privée, et donc plus respectueux de la dignité humaine - comme le recours à un traitement de donnée biométrique qui ne laisse pas de traces ou comme le port de la donnée biométrique sur un support détenu par la personne concernée - auraient pu être envisagés.

Il ne faut pas oublier que les personnes concernées viennent pour leur loisir et/ou leur remise en forme sur le site du requérant ; le requérant envisage qu'à court et à moyen termes, le traitement envisagé intègre les données – notamment biométriques – de 7.000 personnes.

Il n'est pas exclu que des personnes mal intentionnées seront forcément intéressées de posséder une telle base de données comportant 7.000 empreintes digitales pour des raisons très différentes et attentatoires aux droits de ces abonnés.

Par conséquent, et compte tenu de toutes ces considérations, la Commission nationale estime que le traitement pris dans son ensemble n'apparaît ni adapté ni proportionné aux objectifs poursuivis.

Pour éviter tout malentendu, la Commission relève que, même dans l'hypothèse où le traitement envisagé serait légitime parce que le consentement serait exprès, non équivoque, libre, spécifique et informé au sens de l'article 10 paragraphe (1) lettre (a), elle ne pourrait pas accorder l'autorisation sollicitée du fait du non respect du principe de proportionnalité tel que défini à l'article 4 de la loi.

4. Mesures de sécurité prévues aux articles 22 et 23 de la loi

L'ensemble des mesures de sécurité doit conférer un « niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger » (cf. document parlementaire 4735/13, p.37 et Directive 95/46/CE, article 17, paragraphe 2).

Ces mesures doivent également viser à prévenir tout autre risque d'atteinte aux données tel que leur vol, leur effacement, etc., ainsi que tout risque d'utilisation pour d'autres finalités (cf. avis d'initiative de la Commission belge pour la protection de la vie privée relatif aux traitements d'images effectués en particulier par le biais de systèmes de vidéosurveillance, n° de rôle 34/99 du 13/12/1999).

C'est au requérant de prouver qu'il met en place un niveau de sécurité approprié.

En l'espèce, les mesures de sécurité prévues aux articles 22 et 23 de la loi ont fait l'objet d'une description. Compte tenu du caractère sensible du traitement envisagé et des interrogations qui subsistaient, la Commission nationale s'est rendue sur place le 28 novembre 2005 avec l'aide d'un consultant informatique de la société Telindus PSF S.A.

Le requérant utilise le système 'macX System' de la société EWV Kontrollsystem, qui est un système propriétaire. Le requérant n'a pas donné d'indication sur l'encryptage (gestion des clés) sur laquelle repose la sécurité du système.

Il convient de relever également que le requérant n'a pas de certification de qualité comme, par exemple, la norme ISO9001. Il ne se réfère pas non plus à une norme pour la gestion de la politique de sécurité des informations (comme, par exemple, la norme ISO 17799) ce qui donnerait aux abonnés l'assurance que les fichiers informatiques sont continuellement protégés. Mais, il faut toutefois reconnaître qu'à ce jour aucun incident au niveau de la sécurité du système n'a été constaté.

La Commission nationale note également que le requérant a exprimé sa volonté de sanctionner tout abus venant, par exemple, d'un client ou d'une personne extérieure qui souhaiterait s'emparer des données à caractère personnel. Pour prévenir de tels abus, le requérant s'appuie aussi sur la confidentialité : ainsi, tous les contrats de travail et tous les contrats des intervenants externes (les « Service Level Agreements », SLA) contiennent une clause relative à la confidentialité.

En outre, le requérant a mis en place dès le 9 décembre 2005 un code de conduite qui concerne exclusivement la sécurité informatique. Ce code reprend, pour l'essentiel, les exigences de la norme ISO 17799.

En conclusion, la Commission nationale considère que le système informatique répond aux critères de sécurité, même s'il n'est pas confirmé par une certification ou un audit externe. Le code de conduite du requérant répond à une politique sécuritaire satisfaisante. La Commission nationale note enfin que pour parvenir à un niveau de sécurité encore plus élevé, le requérant devrait également arrêter une procédure de gestion des incidents.

III. Mesures immédiates

La loi prévoit que la Commission nationale peut prononcer des sanctions administratives à l'égard des responsables de traitement : l'article 33 paragraphe (1) lettre (c) de la loi prévoit ainsi qu'elle peut « interdire temporairement ou définitivement un traitement contraire aux dispositions de (…) la loi ou de ses règlements d'exécution ».

Compte tenu du caractère intrusif du traitement à des fins de surveillance, pour lequel l'autorisation n'est pas accordée, et étant donné que le traitement de données biométriques a d'ores et déjà été mis en œuvre, la poursuite de celui-ci porte atteinte aux libertés et droits fondamentaux des personnes concernées.

Dès lors, la Commission nationale fait interdiction définitive au requérant de poursuivre le traitement décrit dans sa demande du 31 octobre 2005 (numéro R002245/A002062).

Compte tenu des développements qui précèdent, la Commission nationale, réunissant ses trois membres effectifs et délibérant à l'unanimité des voix :

- n'autorise pas le traitement de données à caractère personnel sollicité par le requérant dans sa demande du 31 octobre 2005 (numéro R002245/A002062),
- interdit définitivement au requérant de poursuivre le traitement en question en application de l'article 33 paragraphe (1) lettre (c) de la loi.

Ainsi décidé à Luxembourg en date du 21 décembre 2005

La Commission nationale pour la protection des données

(*s.*) Gérard Lommel	(*s.*) Pierre Weimerskirch	(*s.*) Thierry Lallemang
Président	Membre effectif	Membre effectif

Délibération n°33/2006 du 12 avril 2006 de la Commission nationale pour la protection des données relative à la demande d'autorisation préalable introduite par l'établissement public Domaine Thermal de Mondorf en matière de traitement à des fins de surveillance contenant des données biométriques.

I. Procédure et forme de la demande

L'établissement public de droit luxembourgeois du Domaine Thermal de Mondorf (ci-après désigné « le requérant »), établi et ayant son siège à L-5601 Mondorf-les-Bains, avenue des Bains, a introduit en date du 1er mars 2006, une demande d'autorisation par l'intermédiaire de son avocat, Maître Cyril Pierre-Beausse, enregistrée sous les références R002445 / A002211, sur base de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après en abrégé « la loi »).

La Commission nationale pour la protection des données (ci-après « la Commission nationale ») constate que le requérant s'est désigné lui-même comme responsable du traitement.

La Commission nationale se déclare compétente pour examiner la demande d'autorisation sur base des articles 3, 10, 14, paragraphe (1), lettre (a) et 32, paragraphe (3), lettre (d), de la loi.

La demande d'autorisation est recevable, étant donné que celle-ci contient toutes les informations obligatoires mentionnées à l'article 14, paragraphe (2), de la loi.

Cette demande intervient suite à la délibération n°89/2005 de la Commission nationale notifiée en date du 21 décembre 2005. Par demande du 31 octobre 2005, enregistrée sous les références R0002245 / A002062, le requérant avait, en effet, demandé à la Commission nationale l'autorisation de pouvoir recourir à un traitement de données à caractère personnel à des fins de surveillance. Ce traitement prévoyait la constitution d'une base de données centralisée contenant des données biométriques, à savoir les gabarits des empreintes digitales des abonnés au service « Le Club ». La Commission nationale n'avait pas autorisé ce traitement parce que le requérant ne justifiait pas de raisons impérieuses de sécurité ou de protection de l'activité exercée dans les locaux à protéger susceptibles de justifier le recours à un tel traitement.

II. Objet de la demande et bien-fondé

Description du traitement envisagé

Le requérant entend mettre en place un système d'accès à ses installations réservé à ses clients abonnés au service « Le Club » (ci-après, les abonnés).

Lors de l'enregistrement de son abonnement, le futur abonné doit fournir à l'hôtesse d'accueil un ensemble de données déterminées : il se fait photographier et remet ses données d'identification (nom, prénom, adresse, téléphone), ses données bancaires et deux données biométriques, à savoir une image de deux empreintes digitales, de préférence une de chaque main.

Pour enregistrer lesdites données biométriques, le futur abonné doit déposer successivement deux de ses doigts sur un numériseur qui capte l'image de chaque empreinte. Le logiciel du système informatique extrait ensuite des minuties. Une minutie est l'arrangement particulier des lignes papillaires formant des points caractéristiques à l'origine de l'individualité des dessins digitaux (ex. arrêt de lignes, bifurcations, lacs, îlots, points). Le logiciel va ensuite calculer, à partir des minuties, une valeur de contrôle grâce à une formule algorithmique ; cette valeur est une suite numérique qui est appelée gabarit ou valeur de référence. L'image de l'empreinte est, dès lors, transformée en gabarit. Le logiciel renouvelle cette opération avec la seconde empreinte digitale.

Les gabarits en question sont transmis par fréquence radio sécurisée à l'une des deux puces du bracelet-chip dans laquelle ils resteront stockés. Le bracelet-chip reste en la possession exclusive de l'abonné pendant toute la durée de l'abonnement.

Le processus relatif aux empreintes digitales ci-avant décrit constitue l'enrôlement. Suivant la demande, les images des deux empreintes digitales ne sont pas enregistrées pendant cette phase.

Le bracelet-chip contient deux puces électroniques distinctes et autonomes qui ont chacune une fonctionnalité propre.

Sur une de ces deux puces, figurent uniquement les gabarits ci-avant décrits des empreintes digitales de l'abonné détenteur dudit bracelet. Ces données ne sont pas stockées dans une base de données centralisée.

Sur la seconde puce, est enregistré le numéro d'identification de l'abonné qui possède le bracelet-chip. Cette puce permet aussi l'ouverture des casiers des vestiaires. Ce numéro d'identification permet de faire le lien avec les données de la base centralisée du requérant, dans laquelle figurent le numéro d'identification de l'abonné, une photographie, ses données d'identification (nom, prénom, adresse, téléphone), ses données bancaires ainsi que le décompte des services reçus par l'abonné sur le site.

L'abonné, qui souhaite accéder aux installations du requérant, se présente avec son bracelet-chip devant les bornes qui lui sont réservées près des tourniquets : il présente son bracelet-chip devant la borne.

Ensuite, il va placer un des deux doigts choisis lors de l'enrôlement sur le capteur se trouvant sur la borne laquelle contient le même logiciel informatique que celui utilisé lors de l'enrôlement. Le logiciel va appliquer la même formule algorithmique à l'empreinte digitale captée. Le système informatique de la borne va ensuite comparer le gabarit qu'il vient d'obtenir avec chacun des deux gabarits sauvegardés dans le bracelet-chip.

Si la comparaison est positive avec un des deux gabarits en question, alors le tourniquet se débloque et l'abonné a accès aux installations du site du requérant.

Il convient de préciser encore qu'à l'instar du processus d'enrôlement, l'image de l'empreinte digitale captée à la borne n'est pas enregistrée dans le système.

A l'expiration de la validité de son abonnement, la personne concernée choisit, soit de renouveler, soit de mettre fin à son abonnement. Dans la première hypothèse, la personne concernée conserve son bracelet-chip avec les gabarits et le numéro d'identification qui restent sauvegardées. Dans la seconde hypothèse, le requérant récupère le bracelet-chip et efface toutes les données qu'il contient. Dans ce dernier cas, si la personne souhaite, plus tard, souscrire un nouvel abonnement au Club, elle devra renouveler les opérations d'enrôlement ci-avant décrits.

A. Généralités : l'applicabilité de la loi

Les traitements contenant des données biométriques ne sont pas expressément prévus par la loi du 2 août 2002. Par conséquent, il y a lieu de vérifier, à titre préliminaire, si ladite loi a vocation à s'appliquer.

Donnée biométrique et donnée à caractère personnel

Il se pose la question de savoir si une donnée biométrique répond à la définition de donnée à caractère personnel telle qu'elle figure dans la loi du 2 août 2002.

La biométrie est « l'exploitation automatisée de caractéristiques physiologiques ou comportementales pour déterminer ou vérifier l'identité » (IBG, International Biometric Group). La biométrie est donc la transformation des caractéristiques physiques d'un individu en une suite numérique.

Il a été précisé que les systèmes biométriques sont « des applications permettant l'identification automatique ou l'éligibilité d'une personne à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main, etc.), de traces (ADN, sang, odeurs), ou d'éléments comportementaux (signature, démarche) » (CNIL, 22e rapport d'activité 2001, « un siècle de biométrie »).

L'article 2, lettre (e), de la loi définit la donnée à caractère personnel comme « toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable (" personne concernée") ; une personne physique ou morale est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ».

En France, la Commission Nationale de l'Informatique et des Libertés (ci-après : CNIL) a estimé que « par nature, un élément d'identification biométrique ou sa traduction informatique sous forme de gabarit constitue une donnée à caractère personnel entrant dans le champ d'application des lois « informatique et libertés » comme d'autres données personnelles (un nom, une adresse, un numéro de téléphone, etc.). La finalité de ces techniques consiste en effet, pour l'essentiel, à reconnaître une personne physique, à l'identifier, à l'authentifier, à la repérer » (CNIL, 22e rapport d'activité 2001, p.166).

Le Tribunal de Grande Instance de Paris suit cette définition : dans un jugement du 19 avril 2005 (CE Effe Services, Syndicat Sud Rail c/ Effia Services), il a ainsi décidé qu'une « empreinte digitale, même partielle, constitue une donnée biométrique morphologique permettant d'identifier les traits spécifiques qui sont uniques et permanents pour chaque individu ».

En l'espèce, le gabarit de l'empreinte digitale figure dans l'une des deux puces du bracelet-chip appartenant au requérant et qui est en la possession de la personne concernée pendant la durée de l'abonnement.

Par conséquent, et au vu des développements ci-avant exposés, le gabarit d'une empreinte digitale est une donnée à caractère personnel telle que définie par la loi du 2 août 2002.

Le traitement de données au sens de la loi et le traitement de données biométriques

Il convient de déterminer si un traitement contenant une ou plusieurs donnée(s) biométrique(s) est un traitement au sens de la loi.

L'article 2, lettre (s), de la loi donne une définition précise de la notion de traitement de données à caractère personnel.

« Lorsque le traitement des données biométriques suppose la conservation et le stockage des gabarits, il y a constitution d'une base de données qui relève alors de l'ensemble des dispositions des lois de protection des données au premier rang desquelles figurent le principe cardinal de la finalité et le principe implicite de nos législations qui en est le corollaire : le principe de proportionnalité » (CNIL, 22e rapport, p.167). Il échet de préciser que la définition de traitement qui figure dans la loi du 2 août 2002 est identique à celle donnée à l'article 2, paragraphe (3) de la loi française coordonnée n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La solution donnée par la CNIL, autorité de contrôle nationale française, est transposable à notre législation.

La Commission nationale considère, dès lors, que le traitement de données biométriques envisagé par le requérant est à qualifier de traitement de données à caractère personnel et la loi du 2 août 2002 a vocation à s'appliquer.

La qualification du traitement envisagé par le requérant

L'article 2, lettre (q), de la loi définit la surveillance comme « toute activité faisant appel à des moyens techniques en vue de détecter, d'observer, de copier ou d'enregistrer des mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile ».

Il ressort des travaux parlementaires que « le projet de loi [n°4735] inclut les traitements de données à des fins de surveillance comme par exemple la vidéosurveillance ainsi que toute forme de surveillance électronique » (n°4735/0 p.36 et 4735/13 p.97).

La doctrine a retenu que la surveillance des mouvements vise « tous les dispositifs permettant de détecter les mouvements des personnes. Outre les caméras, tombent dans cette catégorie des détecteurs de mouvements, à condition toutefois qu'ils permettent d'identifier, directement ou non, une personne. Sont surtout visés ici les (…) portiques et points de passage qui identifient les personnes qui les franchissent » (La Protection des données personnelles, Cyril Pierre-Beausse, éd. Promoculture, n°162).

En l'espèce, le système décrit dans la demande d'autorisation, utilise une borne d'accès qui détecte et enregistre les mouvements des abonnés voulant accéder aux installations du « Club ».

Par conséquent, il s'agit d'un traitement à des fins de surveillance qui tombe dans le champ d'application de l'article 10 de la loi.

B. Légitimité du traitement envisagé

La Commission nationale note qu'un traitement à des fins de surveillance (que ce soit le régime général visé à l'article 10 ou le régime particulier prévu à l'article 11) doit, pour être licite, être effectué conformément aux dispositions de l'article 4 de la loi (cf. document parlementaire 4735/13, p. 17).

Dérogeant à l'article 5 qui traite des conditions de légitimité générales, l'article 10 de la loi détermine les hypothèses dans lesquelles une surveillance peut être effectuée, lesquelles sont au nombre de trois (cf. document parlementaire 4735/13, p. 17). Les cas d'ouverture permettant cette surveillance sont limitatifs (cf. document parlementaire 4735/00, p. 98).

La Commission nationale retient qu'en procédant de la sorte, le législateur a entendu effectuer lui-même la mise en balance des intérêts respectifs en précisant dans le texte même des articles 10 et 11 de la loi les circonstances dans lesquelles une surveillance est légitime. Il a donc jugé que dans tous les autres cas l'intérêt ou les droits et libertés fondamentaux de la personne concernée prévalent.

En l'espèce, le requérant indique dans sa demande d'autorisation qu'il renvoie à la condition de légitimité exposée dans sa demande d'autorisation du 31 octobre 2005 (ci-après : « la première demande d'autorisation »).

Le requérant y invoquait l'article 10, paragraphe (1), lettre (a), parce « que les personnes concernées donnent leur consentement à la collecte et au traitement des Données, et en particulier des Points de Comparaison ». Il précise que le consentement, « recueilli lors de la souscription à un abonnement » est « (a) informé, au moyen de la brochure [explicative] ; (b) spécifique, car les conditions générales ne sont applicables qu'à l'accès au Site et les Points de Comparaison sont exclusivement utilisés en vue de la Vérification ; et (c) libre, car celle-ci peuvent choisir un mode d'accès au Site autre que l'abonnement, et ainsi ne pas être soumis à la Vérification. »Dans sa demande du 1er mars 2006, le requérant précise aussi que « l'existence du consentement pourra être déduite de l'acceptation par l'abonné de fournir son empreinte digitale ». Il indique encore que l'abonné se verra systématiquement remettre une brochure explicative qui contiendra les informations relatives au fonctionnement du traitement envisagé ainsi que les mentions exigées par l'article 26, paragraphe (1), de la loi.

La notion de consentement figurant à l'article 2, lettre (c), de la loi est plus rigoureuse que celle donnée par la directive 95/46/CE : la loi définit en effet le consentement comme « toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée (…) accepte que les données à caractère personnel fassent l'objet d'un traitement. »

Il convient d'analyser si les éléments constitutifs du consentement tels que définis à l'article 2, lettre (c) de la loi sont effectivement réunies en l'espèce :

- Un consentement spécifique et informé

Tout d'abord, « le consentement doit être spécifique, en ce qu'il ne peut porter que sur des traitements déterminés. C'est dans cette optique que le responsable du traitement doit informer la personne concernée sur la ou les finalités déterminées du traitement auquel les données sont destinées. Si plusieurs finalités sont poursuivies par un même traitement, le responsable du traitement doit en informer la personne concernée. » (cf. Doc. Parl. 4735/13).

Ensuite, le consentement doit être informé. Le droit à l'information est une notion essentielle de la loi. Il s'agit, en plus, d'une obligation de résultat, de sorte qu'en cas de contestation, le requérant devra rapporter la preuve que la personne concernée a été informée (travaux parlementaires, 4735/13, page 24) et qu'il a respecté scrupuleusement cette obligation.

« La personne concernée doit donner son consentement en connaissance de cause, ce qui explique une nouvelle fois le lien entre le consentement de la personne concernée avec le principe de la qualité des données prévu à l'article 4, paragraphe (1) lettre (a), et avec le droit à l'information prévu à l'article 26. Ce droit à l'information doit s'exercer soit lors de la collecte des données auprès de la personne concernée, soit lors de l'enregistrement ou la première communication à un tiers pour les données qui n'ont pas été collectées auprès de la personne concernée. » (cf. Doc. Parl. 4735/13).

En d'autres mots, la personne concernée doit avoir été préalablement rendue attentive et renseignée sur tous les aspects du traitement afin de pouvoir donner son consentement en pleine connaissance de cause.

En vertu de l'article 10, paragraphe (2), et l'article 26, paragraphe (1), de la loi, le responsable du traitement doit informer les personnes concernées de la mise en œuvre de la surveillance.

Le droit à l'information, tel qu'arrêté à l'article 26 de la loi, implique que la personne concernée soit informée de ce qui suit :

« (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 ; (…)
- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données ;
- la durée de conservation des données ».

Il convient d'apprécier in concreto la liste des informations supplémentaires telles que prévues à la lettre (c) : « le responsable du traitement devra [en effet] fournir toutes les informations supplémentaires nécessaires compte tenu des circonstances particulières dans lesquelles les données sont collectées, pour assurer à l'égard de la personne concernée un traitement loyal des données, c'est-à-dire une information pleine et entière. La liste de ces informations supplémentaires n'est pas exhaustive. » (travaux parlementaires, 4735/13, page 24).

La Commission estime que, compte tenu de la nature sensible des données biométriques, l'information doit également porter sur l'existence et la catégorie de destinataires à qui les données sont communiquées ainsi que sur la durée de conservation des données et sur l'existence du droit d'accès. Le requérant doit également informer les personnes concernées sur le fait que la donnée biométrique n'est à aucun moment enregistrée dans une base de données.

En outre, « le principe d'un traitement loyal des données à caractère personnel suppose que la personne concernée soit informée des aspects du traitement qui sont pertinents pour elle. Les propriétés du système qui reposent de façon inhérente sur des probabilités et donc sont faillibles, constituent un tel aspect pertinent. Aussi, il revient au responsable du traitement d'informer la personne concernée sur ce fait et sur ce qu'elle peut faire si elle est victime de ce système. Toute présomption d'infaillibilité est erronée » (Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, février 2005, Conseil de l'Europe, extrait n°31). En effet, le résultat d'une comparaison est toujours une estimation. La personne concernée doit, dès lors, être informée lors de la collecte qu'il existe un pourcentage d'échec de reconnaissance de son gabarit. Dès lors, la Commission nationale considère que le requérant doit également informer les personnes concernées de la possibilité que leur donnée biométrique ne soit pas reconnue lors de l'opération de comparaison des gabarits.

Le requérant a indiqué que les nouveaux abonnés se voient systématiquement remettre une brochure explicative.

La Commission nationale estime que la notice d'information doit être remise avant la souscription à l'abonnement, respectivement concomitamment à la souscription. La brochure doit satisfaire aux remarques ci-avant exposées.

Sous réserve des observations ci-avant formulées, le consentement, collecté tel que décrit dans la demande, peut être considéré comme spécifique et informé au sens de la loi.

- - Un consentement exprès et non équivoque

« Le consentement de la personne au traitement de ses données doit être exprès et non équivoque. Aucune forme écrite et aucune formule sacramentelle ne sont requises. » (cf. Doc. Parl. 4735/13).

Il en résulte qu'un consentement implicite ou tacite ne répond pas aux exigences de la loi et n'est pas suffisant pour légitimer un traitement de données, dès lors qu'il est dépourvu d'une manifestation de volonté active et spécifique.

Le préposé du requérant devra donc recueillir directement le consentement exprès et non équivoque de chacun des abonnés.

- - Un consentement libre

Il ressort des travaux parlementaires que les articles 1112 et suivants du Code civil doivent servir de lignes directrices pour apprécier le caractère libre du consentement (cf. doc. parl. 4735/13, p.5). Ils précisent encore que « la liberté du consentement doit s'apprécier au cas par cas au regard des circonstances de l'espèce ».

La doctrine retient que « l'utilisation de la biométrie doit demeurer volontaire. Le consentement doit être libre, spécifique et informé. Cela suppose que le consommateur (la personne concernée) ait à disposition d'autres alternatives s'il ne souhaite pas que des données biométriques le concernant soient collectées et traitées. (…) Le consentement sera en particulier libre si elle [la personne concernée] n'éprouve pas de réticence par rapport à l'utilisation des données biométriques la concernant. Lorsqu'il n'est pas possible d'obtenir un consentement libre, notamment lorsque la personne concernée se trouve dans une situation de subordination ou dans un rapport déséquilibré qui ne lui laisse pas de véritable choix, (…) le recours à la biométrie ne peut intervenir que si la loi le prévoit… » (Quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé, Jean-Philippe Walter, 26e Conférence internationale des Commissaires à la protection des données et à la vie privée, septembre 2004, p.8).

La contrainte (sous laquelle le consentement peut être recueilli) peut donc résulter de la situation juridique ou économique dans laquelle se trouve la personne concernée par rapport au responsable du traitement.

En l'espèce, les abonnés qui refusent de remettre leurs données biométriques ont la possibilité d'accéder aux installations du « Club » en payant plus cher ses services (par exemple en achetant une entrée journalière ou un carnet à entrées multiples). Le requérant offre donc une alternative aux personnes qui ne souhaitent pas souscrire un abonnement et fournir leurs données à caractère personnel.

Dès lors, la Commission nationale considère que le consentement de chaque abonné est libre au sens de la loi.

En conclusion, elle estime que la demande du requérant peut être légitimée sur base de l'article 10, paragraphe (1), lettre (a), de la loi sous réserve des observations qui précèdent.

C. Qualité des données

1. La finalité du traitement

Dans sa demande d'autorisation, le requérant renvoie aux finalités du traitement décrites dans sa première demande d'autorisation. Ces finalités étaient alors décrites de la manière suivante :

> « (i) le contrôle de l'accès au Site et la lutte contre la fraude et
>
> (ii) une gestion commerciale optimisée du Site, pour le décompte des entrées sur le compte des Abonnés »

Aux termes de l'article 4 paragraphe (1) lettre (a) de la loi, le responsable du traitement doit s'assurer que les données sont « collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ».

Il est vrai que la fraude peut avoir des conséquences préjudiciables, et peut ébranler la pérennité économique d'une exploitation. En effet, d'une part, l'exploitant est contraint de répercuter le coût que représente pour lui la fraude sur les personnes qui profitent licitement de son installation : le prix des prestations est ainsi majoré pour compenser les pertes financières causées directement par la fraude. D'autre part, la tolérance de la fraude donne une mauvaise image du professionnel : plus la fraude est facile, plus elle incite également les contrevenants à revenir et cela ouvre des perspectives à des personnes mal intentionnées qui voudraient profiter illicitement des installations. Dès lors, la volonté d'éliminer les risques de fraude rassure également les personnes qui ne fraudent pas et qui payent leurs prestations sans poser de difficultés.

Le requérant a donc un intérêt économique évident à profiter de l'évolution technologique pour combattre la fraude et optimiser le fonctionnement de son entreprise.

Les impératifs légitimes qu'il avance sur le plan de la gestion commerciale comprend tant la recherche du confort des abonnés qui se rendent dans les installations que la réduction des coûts économiques liés à la diminution du personnel qui contrôlaient physiquement les flux des personnes entrant dans le site, et plus particulièrement, le flux des abonnés.

Au vu de ce qui précède, la Commission nationale considère que les finalités invoquées par le requérant sont déterminées, explicites et légitimes au sens de l'article 4, paragraphe (1), lettre (a), de la loi.

Elle rappelle toutefois que, conformément à l'article 4 de la loi précitée, l'utilisation des données traitées doit se limiter aux finalités pour lesquelles elles ont été collectées.

2. Proportionnalité

Selon le principe de proportionnalité, tout traitement des données doit être proportionné aux finalités poursuivies. Ce principe implique que le responsable du traitement doit limiter le traitement à des données adéquates, pertinentes et non excessives au regard des finalités à atteindre (cf. article 4, paragraphe (1), lettre (b), de la loi).

a. Catégories de données et traitement envisagé

Dans le cas spécifique des traitements de données biométriques, il est retenu que « la biométrie, à l'instar de toutes les technologies, est définie par son usage. Les technologies biométriques ne sont, en elles-mêmes, ni nécessairement préjudiciables ni nécessairement favorables à la protection de la vie privée. L'application de ces technologies soulève néanmoins plusieurs problèmes de protection de la vie privée particuliers » (Groupe de travail sur la sécurité de l'information et la vie privée, Technologies fondées sur la biométrie, OCDE, 10 juin 2005, p.13).

En effet, « une mesure biométrique est plus qu'un identifiant numérique [car elle] livre des informations personnelles intimes sur la composition de notre corps et sur notre comportement en général » (Commission d'accès à l'information du Québec, La biométrie au Québec : les enjeux » Document d'analyse, juillet 2002).

Par conséquent, les personnes concernées doivent physiquement se soumettre à chaque passage pour s'identifier. De plus, les données biométriques sont collectées à partir du corps humain.

Il convient de souligner que « l'intégralité du corps humain et la manière dont il est utilisé par la biométrie constituent un aspect de la dignité humaine » (Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, Conseil de l'Europe, février 2005, point n°9).

Le Professeur Roger Clarke de l'Australian National University, estime aussi que le recours à la biométrie présente des dangers particuliers pouvant être regroupés en deux catégories. La première est inhérente aux menaces liées à tous les systèmes informatiques (collecte des données sur les individus, multiplication des informations sur leur comportement, leurs déplacements, les actions…), la seconde "s'attache aux caractéristiques propres à la biométrie : celle-ci donne une information intrinsèquement liée à la personne elle-même (distinction entre "information about the person" et "information of the person") ; la personne doit se soumettre physiquement au processus de vérification. Dès lors, la personne concernée doit coopérer : elle doit physiquement se soumettre à la surveillance.

Du fait de l'intrusion particulière dans la sphère privée, qu'elle implique parfois même une atteinte à la dignité humaine et afin de ne pas banaliser son recours, « la biométrie ne doit pas être utilisée seulement parce qu'elle est pratique, mais parce qu'elle constitue le seul moyen d'atteindre le résultat recherché » (Rapport d'information n°439 du Sénat, session 2004-2005, sur la nouvelle génération de documents d'identité et de la fraude documentaire, p.92).

En d'autres mots, « le risque le plus actuel de la généralisation du recours à la biométrie est sa banalisation et la tentation de la substituer à d'autres outils de sécurisation tout aussi performants pour des usages précis » (Pierre Leclercq, A propos de la biométrie, Revue Communication, LexisNexis de mars 2003, p.14 à 18).

Il existe, en effet, un danger supplémentaire lié au traitement contenant des données biométriques : les applications, les risques et les techniques de ces traitements sont mal apprivoisés alors qu'ils resteront longtemps en développement. En l'état actuel des avancées technologiques, toutes les implications des traitements contenant des données biométriques ne sont pas connues.

Dès lors, « des données biométriques ne doivent être utilisées que si leur utilisation est adéquate, pertinente et non excessive, ce qui implique une évaluation rigoureuse de la nécessité et de la proportionnalité des données traitées » (Document de travail sur la biométrie, du 1er août 2003, Groupe de travail « Article 29 » sur la protection des données, n°12168/02/FR GT 80, p.8).

Le degré d'intrusion dans la vie privée diffère en fonction du traitement de données biométriques choisi : il existe en effet une diversité de traitements possibles de données biométriques qui sont plus ou moins intrusifs dans la vie privée des personnes concernées.

La Commission nationale doit dès lors vérifier ci-après si le traitement envisagé par le requérant est proportionné par rapport aux buts recherchés. Il convient de rappeler que la Commission a pour mission de contrôler la proportionnalité des traitements soumis à son autorisation. La jurisprudence luxembourgeoise retient à cet effet que « la CNPD doit nécessairement procéder à un contrôle de la proportionnalité des mesures envisagées pour décider si le traitement ainsi préconisé est nécessaire pour assurer les besoins prévus par la loi » (Cour administrative, 12 juillet 2005, rôle 19234 C).

- Les catégories de données décrites par le requérant dans sa demande d'autorisation

A ce sujet, la demande du requérant renvoie à sa première demande d'autorisation qui indiquait ce qui suit :

> « Les catégories de Données qui n'ont pas de rapport direct avec la surveillance (c'est-à-dire, les données nécessaires au traitement commercial) ne sont pas détaillées ici et font l'objet d'une notification séparée. Les seules Données pertinentes dans le contexte de la présente demande sont les Points de Comparaison. (…) ».

La Commission nationale ne partage pas cet avis, alors qu'elle considère que les données d'identification font également partie du traitement contenant les données biométriques.

- La spécificité de l'empreinte digitale comme donnée biométrique

La CNIL a retenu que « l'empreinte digitale est presque aussi redoutable que les traces ADN car elle est omniprésente : où que l'on aille, il est impossible de ne pas laisser de traces de sa présence ».

A « la différence d'autres données biométriques, [les empreintes digitales] laissent des traces qui peuvent être exploitées pour l'identification des personnes et que dès lors toute base de données d'empreintes digitales est susceptible d'être utilisée à des fins étrangères à sa finalité première » (CNIL, 21e Rapport d'activité, 2000, p.102).

Le risque de dérive est potentiellement plus élevé quand les données biométriques laissent des traces parce qu'elles peuvent « être exploitées à des fins d'identification des personnes à partir des objets les plus divers que l'on a pu toucher ou eu en main (…) » (Rapport de la CNIL du 9 décembre 2003 relatif à la demande d'avis 859.794, p.5).

Il convient de rappeler que toutes les données biométriques ne laissent pas de traces (par exemple, le contour de la main, l'iris, la rétine). Ces données ne présentent pas les mêmes dangers que les données qui laissent des traces : « une base de données de reconnaissance de la voix, de gabarit d'iris, de rétine ou du contour de la main ne peut en aucun cas être utilisée à d'autres fins que de la reconnaissance et d'authentification des personnes qui se présentent devant le capteur » (CNIL, 22e rapport d'activité 2001, p.168). Dans ce cas, le risque de dérive et de détournement de finalité est, dès lors, sans intérêt.

Par conséquent, et en raison du risque très limité de l'exploitation ultérieure de données biométriques ne laissant pas de traces, les traitements incluant de telles données sont facilement acceptables.

Ainsi, en Grèce, l'«Authority for the Protection of Personal Data » (APPA) a précisé dans sa décision n°9/2003 du 31 mars 2003 qu'elle encourage les traitements qui ne laissent pas de traces (« Operational recommandations encourage taking advantage of " mild" biometric technologies based on characteristics that do not leave any traces »).

Il convient de préciser également que le danger lié à l'utilisation des données à caractère personnel à des fins détournées existe encore lorsque l'image de l'empreinte digitale est transformée en gabarit.

Il est vrai que « la transformation d'une empreinte digitale en gabarit est irréversible, il n'y a aucun risque de reconstitution d'empreinte à partir d'un gabarit » (8e rapport d'activité du Préposé fédéral à la protection des données en Suisse).

Mais une empreinte digitale est très facile à extraire (par exemple sur un verre) : il existe donc un risque qu'une empreinte soit collectée et d'y appliquer un algorithme précis pour voir si le gabarit est reconnu dans la base de données qui utilise cet algorithme, et ainsi obtenir les données à caractère personnel de cette personne.

- La proportionnalité en termes d'opérations de traitement : les données biométriques enregistrées sur un support individualisé

Le requérant avait initialement envisagé un traitement qui reposait sur la centralisation des données biométriques, et plus particulièrement des gabarits des empreintes digitales. Dans la délibération précitée n°89/2005, la Commission nationale avait retenu qu'à défaut de justifier de raisons impérieuses de sécurité ou de protection de l'activité exercée dans les locaux à protéger, le premier traitement envisagé n'était ni adapté ni proportionné aux objectifs poursuivis, à savoir le contrôle de l'accès au site, la lutte contre la fraude ainsi que la gestion commerciale du site relative au décompte des entrées des abonnés.

Le traitement envisagé dans ladite demande du 1er mars 2006 est foncièrement différent. En effet, les gabarits des empreintes digitales ne sont plus centralisés dans une base de données unique contrôlée par le requérant. Désormais, les données biométriques sont stockées dans l'une des deux puces contenues dans le bracelet-chip qui reste en la possession exclusive de l'abonné, c'est-à-dire de la personne concernée par le traitement envisagé par le requérant.

La différence fondamentale entre le premier traitement envisagé et le traitement qui fait l'objet de la demande d'autorisation du 1er mars 2006 est le risque potentiel de réutilisation détournée des données biométriques.

En effet, « la conservation dans un traitement des empreintes digitales est susceptible d'être utilisée à des fins étrangères à la finalité que son concepteur lui avait initialement assignée. En effet, et à la différence d'autres données biométriques (…) les empreintes digitales laissent des traces de chacun de nos gestes les plus quotidiens et peuvent être exploitées à des fins d'identification et de recherche des personnes. Dès lors, une base de données d'empreintes digitales, quelle que soit la finalité initiale de sa constitution, est susceptible d'être utilisée à des fins de police. (…) Quoiqu'il en soit, la connotation policière ne résulte pas uniquement de ce que la prise d'une empreinte digitale est, à l'origine, une technique policière. Elle est bien plus généralement liée à ce que dans la plupart des cas, si ce n'est pas tous, la constitution d'un fichier d'empreintes digitales, même à des fins qui ne sont pas illégitimes, va devenir un nouvel instrument de police, c'est-à-dire un outil de comparaison qui pourra être utilisé à des fins policières, nonobstant sa finalité initiale. Il pourrait presque être soutenu que l'empreinte digitale est (…) une information particulière qui présente un risque réel de relâchement du principe de finalité des fichiers » (Rapport d'ensemble relatif à diverses applications de contrôle d'accès utilisant un dispositif de reconnaissance des empreintes digitales, CNIL, 20 octobre 2000, p.2 et 6).

C'est la raison essentielle pour laquelle les traitements de données biométriques non centralisées dans une base de données unique sont, en principe, autorisés par les autorités de contrôle européennes et par les institutions internationales.

Ainsi, le Groupe de travail « Article 29 » sur la protection des données a pris position sur les deux systèmes : il est « d'avis que l'utilisation, à des fins de contrôle d'accès (…), de systèmes biométriques se référant à des caractéristiques qui ne laissent pas de traces (par exemple la forme de la main, mais non les empreintes digitales) ou de systèmes biométriques se référant à des caractéristiques physiques qui laissent des traces, mais dont les données ne sont pas enregistrées dans une mémoire détenue par une personne autre que la personne concernée (autrement dit, les données ne sont pas mises en mémoire dans le dispositif de contrôle d'accès ou dans une base de données centrale), crée moins de risques pour la protection des libertés et des droits fondamentaux de la personne » (Document de travail sur la biométrie adopté le 1er août 2003, n°12168/02/FR, p.7).

En France, la CNIL accepte les traitements de données biométriques ayant pour but la vérification des personnes uniquement le gabarit d'une empreinte digitale est stocké sur un support individuel exclusivement détenu par la personne concernée et dont celle-ci décide librement de l'utilisation (par exemple, délibérations n°03-015 du 24 avril 2003 et n°2005-115 du 7 juin 2005).

De même, en Suisse, le Préposé fédéral à la protection des données (PFPD) a eu à se prononcer le 6 juin 2005 sur le projet pilote « Secure Chek ». Ce projet a pour but d'améliorer le contrôle de la sécurité des données des passagers et de leurs documents de voyage. Dans le cadre de ce projet, le passager « porteur d'un passeport est authentifié à l'aide de données biométriques (gabarits), ayant été saisies au guichet d'enregistrement après le contrôle du passeport du passager et enregistrées de façon décentralisée sur une carte à puce (smart card) » (Résumé du rapport final du 6 juin 2005). Le PFPD apporte une appréciation positive de l'usage des données biométriques mais précise que « toute modification du projet Secure Check allant dans le sens d'un stockage centralisé des données biométriques ou d'un stockage de données brutes nécessiterait, sous l'angle de la protection des données, une appréciation différenciée, qui n'est pas couverte par le présent rapport ».

Dans son 12ème rapport d'activités 2004/2005, le PFPD recommande de prendre en considération entre autres les principes suivants lors du recours à des données biométriques dans le secteur privé :

> « Il faut privilégier … l'utilisation de données biométriques n'impliquant pas le stockage de gabarits dans une base de données gérée par un responsable de traitement autre que la personne concernée. Cette procédure ne soulève en principe pas de problèmes particuliers du point de vue de la protection des données, dès lors que le gabarit est conservé sur un support dont la personne concernée a l'usage exclusif (carte à puce, téléphone mobile, etc.)

- Si une base de données est constituée et gérée par un responsable de traitement autre que la personne concernée, l'élément biométrique retenu peut avoir des conséquences sur les libertés et droits fondamentaux. Tel est en particulier le cas lorsque l'élément biométrique laisse des traces, comme l'empreinte digitale. Le recours à un tel élément doit répondre à un intérêt prépondérant qualifié de sécurité.

- En l'absence d'un tel intérêt, il convient de recourir à un élément biométrique qui limite le risque d'abus, tel que celui ne laissant pas de trace, comme le contour de la main ».

- Conclusion relative aux catégories de données et opérations de traitement envisagé

En l'état actuel des avancées technologiques, et compte tenu du faible risque de réutilisation des données biométriques stockées exclusivement sur un support individuel qui reste en la seule possession de la personne concernée, la Commission nationale considère que le traitement envisagé dans la demande du 1er mars 2006 susmentionnée apparaît comme adapté et proportionné aux objectifs poursuivis.

b. Catégories de personnes concernées

Il ressort de la demande d'autorisation que les personnes concernées par le traitement envisagé sont les personnes ayant souscrit un abonnement au service « Le Club ».

c. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Le requérant renvoie également à sa première demande d'autorisation dans laquelle il indiquait que les « données ne sont communiquées à aucun tiers en vue d'un autre traitement (…) Il n'y a pas de destinataires externes ».

d. Durée de conservation des données

Conformément à l'article 4, paragraphe (1), lettre (d), de la loi, les données traitées ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

Une durée limitée de conservation de données constitue une garantie supplémentaire pour éviter d'éventuels détournements de finalités.

Dans sa demande, le requérant précise ce qui suit :

> « Lorsque l'abonnement prend fin, le bracelet-chip est désactivé (donc ne permet plus l'accès) mais contient toujours les Minuties. Si la personne concernée (A) renouvelle son abonnement, les Minuties sont conservées et le bracelet-chip est simplement réactivé ; (B) met définitivement fin à son abonnement, le bracelet-chip est restitué au Domaine Thermal et les Minuties sont systématiquement détruites par effacement des données contenus sur le bracelet-chip. »

Le requérant devra veiller à effacer les données biométriques du bracelet-chip à la fin de l'abonnement, respectivement dès que l'abonné l'aura retourné et au plus tard dans les vingt quatre heures. A ce titre, le requérant indique dans sa demande d'autorisation qu'il « va mettre en place une procédure obligatoire pour tous les membres de son personnel affecté à l'accueil du public et à la gestion des abonnements (et chargés à ce titre de l'Enrôlement). »

D. Les droits d'accès et de rectification

Il est acquis que « toute personne peut accéder aux données biométriques qui la concerne (article 8, lettre b, Convention 108). Ce droit s'applique aussi bien aux données biométriques qu'aux données associées qui révèlent, intentionnellement ou non, des informations sur la personne concernée. (…) Accorder le droit d'accès aux données biométriques supposera souvent qu'une machine capable de lire les données biométriques soit à disposition. De même cela pourrait nécessiter un expert pour interpréter et vérifier les données. Le Comité estime que le responsable de traitement ne devrait pas pouvoir refuser de telles demandes au seul motif qu'une machine ou un expert ne dont pas disponibles. (Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, février 2005, extraits 80 à 82).

Compte tenu des développements qui précèdent, la Commission nationale considère que le requérant devra prendre toutes les mesures techniquement possibles pour garantir aux abonnés le droit d'accès à leurs données à caractère personnel.

Ensuite, en vertu du droit de rectification la personne concernée a le droit de demander l'effacement de son gabarit et, corollairement, un nouvel enrôlement de son empreinte digitale dès qu'elle considère que le taux de faux rejets est anormalement élevé.

En effet, la reconnaissance par comparaison de gabarit repose sur la probabilité : « au cours de la phase d'enrôlement, l'algorithme servant à extraire le gabarit de la caractéristique biométrique peut être plus ou moins étendu selon la finalité du système. Un algorithme moins étendu va accroître la probabilité de fausses acceptations ou de faux rejets puisque le gabarit sera moins spécifique.. » (Rapport d'étape, pré.cit., extrait 88). Dès lors, « il est possible qu'un conflit survienne entre le responsable du traitement et la personne concernée à propos du degré acceptable de probabilité de faux rejets. Si la personne concernée demande un nouvel enrôlement alors que le responsable de traitement n'admet pas que les données sont inexactes, le droit de rectification pourrait être interprété comme donnant droit en principe à un nouvel enrôlement par la personne concernée sans coûts excessifs. Il en va de même si des données enrôlées étaient correctes, mais que la caractéristiques biométrique a été modifiée avec l'âge, un accident ou de la chirurgie. Au fil du temps, les données sont devenues graduellement incorrectes » (id. extrait 93).

En tout état de cause, les droits d'accès et de rectification doivent pouvoir être exercés gratuitement par les abonnés lors de la mise en œuvre du traitement envisagé ou à tout moment et sans formalités contraignantes. De plus, ces droits doivent être étendus aux données associées (comme la date et la localisation de l'utilisation du système et les services utilisés) (cf. Conclusions du rapport d'étape pré. cit., point n°7).

E. Pays tiers à destination desquels les transferts de données sont envisagés

Suivant la demande d'autorisation, aucun transfert vers des pays tiers (hors Union Européenne) n'est envisagé.

F. Mesures de sécurité prévues aux articles 22 et 23 de la loi

L'ensemble de ces mesures (de sécurité) doit conférer un « niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger » (cf. document parlementaire 4735/13, p.37 et Directive 95/46/CE, article 17, paragraphe 2).

Ces mesures doivent également viser à prévenir tout autre risque d'atteinte aux données tel que leur vol, leur effacement, etc., ainsi que tout risque d'utilisation pour d'autres finalités (cf. avis d'initiative de la Commission pour la protection de la vie privée belge, n° de rôle 34/99 du 13/12/1999).

C'est au requérant de prouver qu'il met en place un niveau de sécurité approprié.

En l'espèce, les mesures de sécurité prévues aux articles 22 et 23 de la loi ont fait l'objet d'une description détaillée.

La Commission nationale constate que le contenu de la description relative aux mesures de sécurité satisfait aux exigences des prédits articles.

***

Compte tenu des développements qui précèdent, la Commission nationale, réunissant ses trois membres effectifs et délibérant à l'unanimité des voix :

délivre l'autorisation sollicitée en matière de traitement de catégories particulières de données en vertu de l'article 10, paragraphe (1), lettre (a), de la loi ;

autorise, dès lors, le Domaine Thermal de Mondorf à recourir au traitement des données envisagé selon les modalités précisées dans sa demande du 1er mars 2006 sous réserve de respecter les conditions suivantes :

- les données biométriques ne doivent pas être enregistrées dans une base de données centralisée mais stockées exclusivement sur un support individuel qui reste en la seule possession de la personne concernée ;
- la brochure explicative devra être remise aux personnes concernées avant la souscription de l'abonnement, respectivement concomitamment à cette souscription ;
- outre les informations obligatoires prévues à l'article 26, paragraphe (1), de la loi, la brochure explicative et/ou les informations fournies oralement devront contenir les éléments suivants :

- l'existence et la catégorie de destinataires à qui les données sont communiquées ;
- l'existence du droit d'accès et de rectification ;
- l'indication que la donnée biométrique n'est pas enregistrée dans une banque de données ;
- l'existence d'un taux d'erreur de reconnaissance inhérent à tout système incluant des gabarits d'empreintes digitales ;
- la durée de conservation des données à caractère personnel ;

- le Domaine Thermal de Mondorf devra veiller à effacer les données biométriques du bracelet-chip à la fin de l'abonnement, respectivement dès que l'abonné l'aura retourné et au plus tard dans les vingt quatre heures ;
- plus généralement, les données recueillies doivent être traitées loyalement et ne doivent être utilisées que pour les finalités sur lesquelles est fondée la présente autorisation.

Ainsi décidé à Luxembourg en date du 12 avril 2006.

La Commission nationale pour la protection des données

(*s.*) Gérard Lommel	(*s.*) Pierre Weimerskirch	(*s.*) Thierry Lallemang
Président	Membre effectif	Membre effectif

Avis de la Commission nationale pour la protection des données relatif à la numérisation d'actes de l'état civil de la commune de Lintgen par un prestataire de services privé.

Délibération n°136/2006 du 22 décembre 2006

La Commission nationale pour la protection des données a été saisie par courrier de Monsieur le Ministre de l'Intérieur et de l'Aménagement du Territoire du 4 décembre 2006 aux fins d'émettre un avis relatif à un traitement de données à caractère personnel effectué par l'administration communale de Lintgen, consistant en la numérisation, par un prestataire de services privé, d'un certain nombre de registres et d'actes de l'état civil tenus au sein de ladite commune. L'administration communale de Lintgen souhaite obtenir certaines précisions portant notamment sur l'applicabilité des dispositions de la loi du 2 août 2002, relative à la protection des personnes à l'égard du traitement des données à caractère personnel (la Loi). A ce titre, la Commission nationale voudrait formuler les observations qui suivent.

L'organisation de l'état civil a été strictement encadrée par le Code civil. En effet, le livre Premier, Titre II de ce dernier énumère les différents actes de l'état civil et définit leur contenu et mentions. Une analyse de ces dispositions permet de relever que chacun des actes de l'état civil y prévus comprend des données à caractère personnel, au sens l'article 2 lettre (e) de la Loi. Il en ressort en outre, en combinaison aves les dispositions de la loi communale modifiée du 13 décembre 1988, qu'en leur qualité d'officiers d'état civil, le bourgmestre, les échevins ou leurs conseillers spécialement délégués sont tenus de dresser les actes de naissance, de mariages et de décès, afin de leur conférer un caractère authentique et de les transcrire dans les registres.

Considérant que la tenue des registres d'état civil constitue une mission légale pour les officiers de l'état civil, les administrés ne peuvent s'opposer à ce que les informations nécessaires à la rédaction d'un acte fassent l'objet d'un traitement informatique et soient conservés sous cette forme. Il ressort des pièces communiquées par Monsieur le Ministre de l'Intérieur et de l'Aménagement du Territoire à la Commission nationale que la commune de Lintgen envisage de faire numériser tous les actes de l'état civil qu'elle détient pour les années 1900 à 2004.

La numérisation consiste en « la conversion ou transformation d'un objet réel en une suite d'éléments binaires, permettant de représenter cet objet en informatique » et tombe sous la définition d'un traitement de données à caractère personnel (article 2 lettre (s) de la Loi). Il s'agit en l'espèce d'une opération ayant pour objet de transformer des données existantes, conservées sur support papier, en données numérisées. Cette opération est effectuée à l'aide d'un procédé automatisé, appliqué à des données à caractère personnel, comprenant notamment la collecte (scannerisation / numérisation), l'enregistrement (CD), l'organisation (indexation) et la conservation de données. Partant, les dispositions de la Loi s'appliquent au traitement envisagé.

Etant donné que le traitement envisagé peut être considéré comme nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, la condition de légitimité du traitement posée à l'article 5 paragraphe (1) lettre (b) de la Loi se trouve remplie.

Par ailleurs, l'administration communale de Lintgen, en tant que responsable du traitement, doit s'assurer du respect des principes de loyauté et de licéité pour les données qu'elle traite ou les opérations afférentes qu'elle sous-traite. Elle devra notamment veiller à ce que ces données collectées pour les finalités déterminées par le Code civil ne soient pas traitées ultérieurement de manière incompatible avec ces finalités.

La Commission nationale considère que les finalités des traitements relatifs aux registres d'état civil, telles qu'elles résultent du Code civil et de la loi, sont notamment la constitution, la tenue, la consultation, la vérification et la conservation de tels registres. La volonté de numériser ces registres se traduit par une prise en compte de l'administration communale des évolutions techniques récentes en matière informatique et œuvre dans le sens d'un développement d'une administration de proximité plus transparente pour les usagers. La Commission nationale considère qu'une telle numérisation ne constitue pas un traitement ultérieur incompatible avec les finalités décrites ci-avant.

Les données traitées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et, par ailleurs, exactes et mises à jour. En l'espèce, les fichiers numérisés ne comporteront aucune donnée distincte ou additionnelle par rapport aux registres ou actes originaux.

La Commission nationale ne dispose pas d'éléments suffisants lui permettant de connaître l'utilisation des fichiers numérisés par les officiers d'état civil, habilités à consulter les actes et registres. La Commission nationale présume que l'administration communale utilisera seulement les documents sous forme numérisée, d'une part, afin de faciliter les recherches qu'ils devront effectuer dans le cadre de leur mission légale et, plus généralement, de faciliter la gestion des documents de l'état civil. La Commission nationale présume également que les documents originaux restent en l'état et que les documents numérisés ne feront office que de simples archives. Dans l'hypothèse où ces présomptions ne correspondraient pas aux utilisations envisagées par les officiers d'état civil de la commune de Lintgen, la Commission nationale se tient à votre disposition pour fournir, le cas échéant, des précisions complémentaires.

Les fichiers électroniques issus de la numérisation des actes de l'état civil seront sans doute utilisés non seulement par l'officier de l'état civil, mais également par d'autres collaborateurs de l'administration communale, appelés à assister ce dernier dans sa fonction. Dans ce contexte, la Commission nationale aimerait rappeler l'article 21 de la Loi, relatif à la subordination. Il résulte de ces dispositions que les employés ne doivent avoir accès aux données personnelles que dans la mesure où cela s'avère nécessaire à l'accomplissement de la fonction leur confiée sous l'autorité de l'officier de l'état civil et qu'ils ne peuvent « les traiter que sur instruction du responsable du traitement ». De plus, ces opérations de consultation ou d'utilisation des données numérisées ne peuvent se faire que dans le strict respect des finalités pour lesquelles les données sont traitées.

Quant à la durée de conservation des données des registres de l'état civil, la Commission nationale considère que, conformément aux dispositions de l'article 45 du Code civil, le responsable du traitement pourra conserver lesdites données pendant une durée de cent ans, notamment sous forme numérique. Au-delà, les données devront être archivées.

Il ressort du dossier soumis à la Commission nationale que la numérisation des données de l'état civil ne sera pas effectuée par le responsable du traitement, mais par la société de droit français H&E, qui est alors à considérer comme sous-traitant au sens de l'article 2 lettre (p) de la Loi.

Dans le cadre d'une sous-traitance, le responsable du traitement a l'obligation, conformément aux dispositions des articles 21 et 22 de la Loi, de choisir un sous-traitant apportant des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives au traitement à effectuer, ainsi que de lui fournir des instructions relatives au traitement à effectuer. Le responsable doit, en plus, mettre en œuvre toutes les mesures techniques et d'organisation appropriée pour assurer la protection des données qu'il traite notamment contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés. La tenue et la gestion de l'état civil relevant de la responsabilité de l'officier d'état civil, ce dernier devra par conséquent veiller à ce que les conditions de l'article 22 de la Loi soient respectées.

La Commission nationale note que, d'après les termes de l'article 22 paragraphe (3) de la Loi, tout traitement effectué pour compte doit être régi par un contrat ou un acte juridique, consigné par écrit, liant le sous-traitant au responsable du traitement. Ce document doit notamment prévoir que le sous-traitant n'agit que sur la seule instruction du responsable du traitement et que le respect des obligations de sécurité des traitements détaillés à l'article 23 de la Loi lui incombe.

Il ressort des pièces transmises pour avis que le contrat proposé par le sous-traitant énumère les instructions du responsable du traitement (cahier des charges), mais ne mentionne pas expressément l'obligation de veiller à la confidentialité et à la sécurité des données et ne précise aucunement les mesures de sécurité que le sous-traitant doit respecter. Certes, ledit contrat fait référence au secret professionnel et à l'obligation de discrétion. Or, la Commission nationale fait observer que le prestataire de services ne relève pas des professions soumis au secret professionnel au sens de l'article 458 du Code Pénal luxembourgeois.

La Commission nationale recommande dès lors une adaptation dudit contrat, visant à renforcer l'obligation de confidentialité (de nature contractuelle) à laquelle le sous-traitant sera tenu. Les parties en cause devront également détailler les mesures de sécurité particulières qu'elles prennent, au sens de l'article 23 de la Loi, quant au traitement envisagé. Alors même que les données traitées ne sont pas à considérer comme catégories particulières de données au sens de l'article 6 de la Loi (communément appelées « données sensibles »), certaines des données traitées relèvent néanmoins d'une protection spécifique, instaurée par l'article 45 du Code civil, comme par exemple les données relatives à la filiation illégitime ou adoptive. Ces mesures de confidentialité et de sécurité s'imposent donc en l'espèce au vu de la nature des données à caractère personnel qui seront traitées par le sous-traitant.

Il se pose également la question de savoir si les agents (privés) du sous-traitant peuvent ainsi être admis à accéder au contenu des registres de l'état civil de la commune aux fins d'effectuer la numérisation des actes, alors que les dispositions de l'article 45 du Code civil prévoient que les registres de l'état civil datant de moins de cent ans ne peuvent être consultés que par des agents de l'Etat et des communes, ainsi que les personnes munies d'une autorisation écrite du Procureur d'Etat. Le projet soumis à l'avis de la Commission ne pourra dès lors être mis en œuvre qu'à la condition de l'obtention d'une autorisation afférente du Procureur d'Etat près le tribunal d'arrondissement de et à Luxembourg.

Considérant que l'appréciation de l'opportunité d'autoriser ou de refuser la consultation des registres de l'état civil relève de la compétence exclusive du Procureur d'Etat territorialement compétent, la Commission nationale estime ne pas devoir prendre position à ce sujet.

Il résulte des développements qui précèdent que la Commission nationale émet un avis favorable à la mise en œuvre du traitement envisagé, sous réserve que le contrat conclu entre le responsable du traitement et le sous-traitant soit adopté en vue d'assurer le respect des articles 21 à 23 de la Loi et sans réserve des attributions du Procureur d'Etat en la matière.

Ainsi décidé à Luxembourg en date du 22 décembre 2006

La Commission nationale pour la protection des données

(*s.*) Gérard Lommel	(*s.*) Pierre Weimerskirch	(*s.*) Thierry Lallemang
Président	Membre effectif	Membre effectif

Table des Annexes

Feuille Couleur

VI.Programme de travail du « groupe article 29 »

Article 29 Groupe de protection des données

10650/04/FR
WP 92

Programme de travail 2004
Groupe de travail "Article 29"

Adopté le 17 mars 2004

Le groupe de travail a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 14 de la directive 97/66/CE.

Le secrétariat est assuré par la Commission européenne, DG Marché intérieur, Direction E "Services, Droit d'auteur, Propriété Industrielle et Protection des Données", B-1049 Bruxelles - Belgique - Bureau: C100-6/136

Adresse Internet: www.europa.eu.int/comm/privacy

Programme de travail 2004
Groupe de travail "Article 29"

QUESTIONS SECTORIELLES	- Patients et données médicales - Crédit à la consommation et paiements - Protection des données des travailleurs - Qualifications professionnelles	[*] *
APPLICATION ET INTERPRÉTATION DE LA DIRECTIVE	- Simplification des transferts internationaux (règles d'entreprise contraignantes, mise en œuvre plus uniforme de l'article 26, paragraphe premier) - Simplification des exigences de notification - Application - Meilleure harmonisation des obligations d'information - Constatation d'un niveau adéquat de protection Australie - Constatation d'un niveau adéquat de protection Nouvelle-Zélande	* * * *
FLUX DE DONNÉES DANS LE CONTEXTE DE LA CIRCULATION INTERNATIONALE DES PERSONNES	- Constatations d'un niveau adéquat de protection concernant le transfert des données des dossiers passagers (PNR): • États-Unis • Canada • Australie - Initiative communautaire sur les PNR à l'OACI - Système d'information sur les visas - Biométrie	* * * * * * *
QUESTIONS TECHNIQUES	- Administration en ligne - Données génétiques - Systèmes d'identification par radiofréquences (RFID) - Droits de propriété intellectuelle - Task force Internet: - Interprétation de la directive 2002/58/CE et questions relatives à l'application des dispositions, courriels commerciaux non sollicités (spam) - Sécurité dans les réseaux électroniques - Technologies mobiles - Services de géolocalisation - P3P, TCP, authentification en ligne - Questions liées au respect du droit d'auteur - Whois	* * * *
RELATIONS PUBLIQUES	- 7e rapport annuel 2002 - 8e rapport annuel 2003	* *

[*] à achever en 2004

CODES DE CONDUITE	- Code de conduite pharmaceutique - Code de conduite de la FEDMA en matière de marketing direct en ligne - code de conduite de l'AESC	*

Fait à Bruxelles, le 17 mars 2004

Pour le groupe de travail
Le président
Peter Schaar

00862/05/FR
WP 109

Programme de travail 2005
Groupe de travail article 29

Adopté le 14 avril 2005

Programme de travail 2005
Groupe de travail article 29

QUESTIONS SECTORIELLES	- Données médicales et concernant les patients et plus particulièrement les aspects concernant le VIH/SIDA (initiative de la DG SANCO en cours)
	- Dossiers médicaux électroniques
	- Protection des données des travailleurs
MISE EN ŒUVRE ET INTERPRÉTATION DE LA DIRECTIVE	- Contribution au suivi du programme de travail pour une meilleure application de la directive
	- Application plus uniforme du paragraphe 1 de l'article 26
	- Règles d'entreprise contraignantes
	- Contrôle, audit coordonné
	- Contribution du groupe de travail article 29 à la sensibilisation à la protection des données dans l'Union européenne
	- Constat du caractère adéquat de la protection des données en Australie
	- Constat du caractère adéquat de la protection des données en Nouvelle-Zélande
	- Rapport sur l'exécution des décisions relatives aux clauses contractuelles types
	- Rapport sur l'exécution de la décision concernant le Canada
FLUX DE DONNÉES ET MOUVEMENTS INTERNATIONAUX DE PERSONNES	- Biométrie appliquée aux documents d'identité
	- Système d'information sur les visas
	- Conservation des données
	- Autres progrès possibles de la DG JLS dans le cadre du premier pilier
	- Initiative communautaire concernant les données PNR à l'OACI
	- Constat du caractère adéquat de la protection des données PNR lors de leur transfert: - États-Unis (examen conjoint) - Canada - Australie - Autres pays ou organisations
	- Progrès possibles dans le cadre du troisième pilier

QUESTIONS TECHNIQUES	- Services publics en ligne (e-gouvernement)
	- Les RFID dans le secteur de la vente au détail
	- Droits de propriété intellectuelle
	- Interprétation et respect de la directive 2002/58/CE, spams, témoins de connexion (cookies) et logiciels espions
	- Sécurité des réseaux électroniques
	- Technologies mobiles
	- Services de géolocalisation
	- Plate-forme de préférence en matière de protection de la vie privée (P3P), TCP, authentification en ligne
	- Respect des droits d'auteur
	- Protocole Whois
	- Services de courrier électronique
	- Aspect technique de la biométrie
	- Technologies alternatives (PETs)
	- Informatique diffuse, interactions avec l'environnement (ambiance intelligence)
	- PIN – Identification unique
	- Permis de conduire / plaques d'immatriculation
COMMUNICATION	- 8ème rapport annuel relatif à l'année 2004
CODES DE CONDUITE	- Code de conduite dans le domaine pharmaceutique
	- Code de conduite de la FEDMA pour le marketing direct en ligne
	- Code de conduite de l'AESC
	- ESOMAR

Fait à Bruxelles, le 14 avril 2005.

Pour le groupe de travail
Le président
Peter Schaar

VII.Programme de travail du « groupe article 29 »

Article 29 Groupe de protection des données

10650/04/FR
WP 92

Programme de travail 2004
Groupe de travail "Article 29"

Adopté le 17 mars 2004

Le groupe de travail a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 14 de la directive 97/66/CE.

Le secrétariat est assuré par la Commission européenne, DG Marché intérieur, Direction E "Services, Droit d'auteur, Propriété Industrielle et Protection des Données", B-1049 Bruxelles - Belgique - Bureau: C100-6/136

Adresse Internet: www.europa.eu.int/comm/privacy

Programme de travail 2004
Groupe de travail "Article 29"

QUESTIONS SECTORIELLES	- Patients et données médicales - Crédit à la consommation et paiements - Protection des données des travailleurs - Qualifications professionnelles	[*] *
APPLICATION ET INTERPRÉTATION DE LA DIRECTIVE	- Simplification des transferts internationaux (règles d'entreprise contraignantes, mise en œuvre plus uniforme de l'article 26, paragraphe premier) - Simplification des exigences de notification - Application - Meilleure harmonisation des obligations d'information - Constatation d'un niveau adéquat de protection Australie - Constatation d'un niveau adéquat de protection Nouvelle-Zélande	* * * *
FLUX DE DONNÉES DANS LE CONTEXTE DE LA CIRCULATION INTERNATIONALE DES PERSONNES	- Constatations d'un niveau adéquat de protection concernant le transfert des données des dossiers passagers (PNR): • États-Unis • Canada • Australie - Initiative communautaire sur les PNR à l'OACI - Système d'information sur les visas - Biométrie	* * * * * * *
QUESTIONS TECHNIQUES	- Administration en ligne - Données génétiques - Systèmes d'identification par radiofréquences (RFID) - Droits de propriété intellectuelle - Task force Internet: - Interprétation de la directive 2002/58/CE et questions relatives à l'application des dispositions, courriels commerciaux non sollicités (spam) - Sécurité dans les réseaux électroniques - Technologies mobiles - Services de géolocalisation - P3P, TCP, authentification en ligne - Questions liées au respect du droit d'auteur - Whois	* * * *
RELATIONS PUBLIQUES	- 7e rapport annuel 2002 - 8e rapport annuel 2003	* *

[*] à achever en 2004

CODES DE CONDUITE	- Code de conduite pharmaceutique - Code de conduite de la FEDMA en matière de marketing direct en ligne - code de conduite de l'AESC	*

Fait à Bruxelles, le 17 mars 2004

Pour le groupe de travail
Le président
Peter Schaar

Feuille couleur

VII. Avis de la Commission consultative des droits de l'homme relatif au rapport annuel de la CNPD de 2003

Avis de la CCDH sur le rapport annuel 2003 de la Commission Nationale pour la Protection des Données

Selon l'art. 32 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, la CCDH est censée aviser le rapport annuel de la Commission nationale de protection des données.

L'année 2003 est, comme le dit le rapport, « la première année civile entière d'activités » (p.7/24). La CNPD s'est consacrée, au-delà de la réception et du traitement des formalités préalables prévues au chap. III de la loi, de l'information et de la guidance des responsables du traitement, de la formation des relations internationales et de la structuration du nouvel établissement public.

Dans sa partie statistique, la CNPD souligne que « moins de 10% des acteurs concernés ont procédé aux formalités imposées par la loi » et « le nombre total des notifications et demandes d'autorisations soumises à la CNPD ne devrait guère être supérieur à 5-7% des traitements effectifs qui devraient y donner lieu. » Etat, secteur public, entreprises industrielles, artisans, commerçants, professions libérales, mais surtout les petites entreprises et les a.s.b.l. accusent le déficit le plus important en la matière. (cf. 9/24)

Malgré cela, la CNPD constate que ses capacités de traitement étaient dépassées dès le mois d'août 2003. « Cette situation est particulièrement insatisfaisante puisque l'administré ne pourra pas compter voir examiner et trancher sa demande dans un délai raisonnable. » Or 50% de ces dossiers en souffrance concernant le traitement de données sensibles et de santé, 6% des données relatives au crédit et à la solvabilité des personnes, les interconnexions de données et des transferts vers des pays tiers (1%) ou la surveillance sur le lieu de travail par l'employeur (30%).

Au coeur des réflexions et travaux de la CNPD figurent des lois, des projets de loi et des mesures d'exécutions réglementaires, voire des procédures et des fonctionnements des autorités publiques, dans le secteur de la santé, au niveau de l'économie et des activités commerciales, ou bien en matière de communications électroniques et nouvelles technologies « où la protection des libertés et droits fondamentaux des personnes, notamment de leur vie privée, est appelée à rencontrer des enjeux significatifs ». (15/24)

Dans ce cadre, la CNPD a élaboré quatre axes stratégiques.

1. réveiller les consciences et sensibiliser

2. devenir force de proposition et propager des standards de bonne pratique

3. stimuler la vigilance des citoyens

4. encourager l'autodiscipline des acteurs et favoriser la co-régulation

En même temps elle s'est fixée une « road map » en trois étapes pour les six années 2003 - 2008. (16-17/24)

La CNPD constate qu'elle a rencontré des difficultés dans la mise en oeuvre de sa mission légale.

La loi, constate-t-elle, est ambitieuse, mais le contexte est peu propice à sa mise en oeuvre.

Cela est selon la CNPD dû à plusieurs facteurs :

1. une dizaine d'années d'application inconséquente de l'ancien cadre légal

2. le faible niveau de prise de conscience des acteurs et des citoyens

3. la sensibilité accrue des populations et des décideurs aux besoins de sécurité intérieure et extérieure

4. et le ralentissement de croissance économique qui font parfois passer les soucis de protection de la vie privée au second rang (19/24)

S'ajoutent les faibles ressources, notamment humaines, de la CNPD, de sorte que la mise en oeuvre de la loi s'avère difficile.

D'où l'appel de la CNPD à une augmentation de ses moyens et à certaines modifications de la loi, notamment en allégeant certaines formalités administratives, car la CNPD craint que la loi ne demeure en fin de compte et à terme inappliquée. D'où aussi une demande à ce que les conditions soient créées pour que la CNPD puis se consacrer plus fortement à l'information du public et à la responsabilisation des acteurs. (20-21/24)

Conclusions de la CCDH :

La CCDH

- constate le caractère exhaustif du rapport d'activités 2003 de la CNPD

- approuve les orientations stratégiques générales que la CNPD préconise pour la période 2003-2008

- félicite la CNPD pour la manière dont elle met en pratique son souci de la protection des libertés et droits fondamentaux des personnes, notamment de leur vie privée

- soutient son appel à une augmentation de ses moyens pour se consacrer à la fois à un traitement des dossiers dans des délais raisonnables, pouvoir poursuivre son travail de réflexion et informer le public des enjeux et des moyens de mettre en oeuvre la loi du 2 août 2002.

Adopté par la Commission Consultative des Droits de l'Homme dans sa séance du 7 mars 2005


droits
chômage
Bankrott
politique
Dettes

Siège : L-4100 Esch-sur-Alzette
Bureaux : 41, avenue de la gare L-1611 Luxembourg
Tél. : (+352) 26 10 60 -1 Fax : (+352) 26 10 60 -29
www.cnpd.lu