Le collège :
Pierre WEIMERSKIRCH, Gérard LOMMEL et Thierry LALLEMANG

L'administration et le service juridique :
Jacques BECKER, Thomas FRERES, Michel SINNER, Georges WEILAND,
Christian WELTER et Marc MOSTERT (de gauche à droite)

Commission Nationale
pour la Protection
des Données

41, avenue de la gare, L-1611 Luxembourg
Siège : L-4100 Esch-sur-Alzette
téléphone : +352 26 10 60 -1 - Fax : +352 26 10 60 - 29

www.cnpd.lu

Commission Nationale pour la Protection des Données
Rapport Annuel 2007

Commission Nationale pour la Protection des Données

Rapport Annuel 2007

Commission Nationale pour la Protection des Données

Rapport Annuel 2007

Mission

Veiller à l'application des lois qui protègent les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée et leurs données à caractère personnel.

Superviser et assurer la transparence par :

- l'examen préalable des traitements soumis à autorisation ;
- la publicité réalisée au moyen du registre des traitements notifiés ;
- les investigations suite à des plaintes ou de sa propre initiative.

Informer et guider avec :

- la sensibilisation du public aux risques potentiels ;
- les renseignements concernant les droits des citoyens et les obligations des responsables des traitements de données ;
- l'explication des règles légales.

Conseiller et coopérer à travers :

- les avis relatifs aux projets de loi et mesures réglementaires ou administratives ;
- les suggestions et recommandations adressées au gouvernement, notamment au sujet des conséquences de l'évolution des technologies ;
- l'approbation de codes de conduites sectoriels, la promotion des bonnes pratiques et la publication de lignes d'orientation thématiques.

Table des matières

ANNEXES :

Avis et décisions

Participation aux travaux européens

1 Avant-propos

L'année 2007, sans marquer un tournant radical dans l'activité de la Commission nationale pour la protection des données, constitue néanmoins à plus d'un titre une année charnière sur son jeune parcours.

Elle a eu à prendre position sur un certain nombre de dossiers importants (notamment sur les systèmes d'alertes professionnels « Whistleblowing », l'interconnexion de divers fichiers publics, la collecte de données pour l'établissement des cadastres des loyers par les Communes) et a participé activement aux travaux sur le plan européen dans des domaines sensibles (dossiers électroniques de santé ; les mineurs et la protection des données ; décision cadre européen sur la protection des données dans les domaines du 3e pilier ; transmission de données des passagers aériens vers des pays tiers ; etc.) et techniques [e-ticketing ; RFID ; moteurs de recherche Internet ; règles contraignantes d'entreprises (BCR)].

Elle a aussi procédé à quelques investigations et contrôles sur les lieux soit à la suite de plaintes ou demandes de vérification de licéité émanant de citoyens, soit de sa propre initiative dans deux ou trois secteurs particulièrement exposés. Parallèlement la Commission nationale a poursuivi ses efforts au niveau de l'information du public souvent insuffisamment sensibilisé aux risques et peu au fait des droits que la loi accorde aux personnes concernées. Elle essaie aussi de fournir aux entreprises, administrations et autres professionnels une guidance concrète assortie de recommandations pratiques adaptées à leur activité. Elle a surtout coopéré avec un nombre croissant de ministères et d'organismes publics qui l'ont consultée avant d'opérer leurs choix finaux sur des questions susceptibles d'impacter de façon substantielle l'envergure et la mise en œuvre de la collecte et de l'utilisation de données à caractère personnel engendrées par de nouveaux développements opérationnels et législatifs.

L'écoute ainsi rencontrée de plus en plus souvent à un stade précoce du processus de décision gouvernemental ou administratif est ressentie comme l'une des grandes satisfactions enregistrées au cours des derniers mois.

Les deux autres sources de satisfaction sont l'adoption par la Chambre des Députés de la loi du 27 juillet 2007– avec les clarifications qu'elle opère dans le cadre légal (tout en simplifiant considérablement les formalités administratives à charge des responsables des traitements de données), et le renforcement de son cadre de personnel dans le cadre du numerus clausus de la fonction publique approuvé par le gouvernement pour le budget 2008.

La Commission nationale s'efforcera de son côté d'être à la hauteur des attentes de ses interlocuteurs. Elle continuera à apporter un soin qualitatif à son travail et fera preuve d'équilibre dans les avis et prises de position qu'elle est appelée à délivrer dans l'exercice de ses missions légales (assortis le cas échéant de recommandations constructives adaptées à la situation et tenant compte des intérêts en présence).

***

Luxembourg, le 11 avril 2008

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

2 Les activités en 2007

Le travail de la Commission nationale se définit autour de plusieurs axes qui ont marqué ses activités au cours de l'année 2007 :

- le conseil et la guidance des acteurs ;
- la supervision du respect de la loi avec notamment le traitement d'un nombre important de dossiers de notifications et d'autorisations pendant toute l'année ;
- les initiatives d'information et de communication, traduites par la poursuite des efforts d'information et de sensibilisation, et ce aussi bien du grand public que des milieux professionnels et publics ;
- les activités européennes avec la participation aux travaux sur le plan européen.

2.1 Conseil et guidance

2.1.1 Concertation avec les organisations représentatives sectorielles, les principaux acteurs économiques, l'Etat et les organismes publics

La Commission nationale a poursuivi sa politique de dialogue et de concertation avec les acteurs publics et privés, que ce soit à propos de questions spécifiques touchant un secteur ou de projets poursuivis par un département ministériel ou, de façon plus générale, afin d'échanger ses vues au sujet de l'application des principes de la protection des données dans les pratiques et procédures usuelles des activités considérées.

Comme par le passé, elle a régulièrement participé aux travaux du Comité National d'Ethique de Recherche (CNER) et du Comité National pour la Simplification Administrative en faveur des Entreprises (CNSAE), et fourni ses recommandations à maintes reprises.

Sur divers dossiers elle était en outre en contact avec les ministères suivants : ministère des Affaires étrangères et de l'Immigration, ministère des Finances, ministère des Transports, ministère de l'Education nationale et de la Formation professionnelle, ministère du Logement, ministère de la Santé ; ainsi qu'avec diverses administrations et organismes publics comme le Centre de Recherche Public (CRP) Henri Tudor et CRP Santé, avec le Médiateur, avec l' « Ombudskomitee fir d'Rechter vun de Kanner », avec la Banque Centrale, etc.

Une importance particulière revient également aux échanges de vues avec la direction du Centre Informatique de l'Etat, le ministère de la Fonction publique et de la Réforme administrative et sa cellule E-Lëtzebuerg.

Le nombre de réunions avec le secteur public (56 contre 32 l'année précédente) s'est ainsi accru en parallèle avec celui des entrevues avec les représentations d'importantes entreprises privées nationales et multinationales et leurs organisations représentatives (du secteur financier notamment) ce qui traduit l'accent mis sur les efforts de promotion des bonnes pratiques et de guidance constructive. Le nombre de réunions avec le secteur privé a été de 40 pour 2007.

2.1.2 Séances d'information, conférences, exposés

En 2007, la Commission nationale a assuré 14 séances d'information, de conférences et d'exposés contre 11 en 2006.

Un accent particulier a été mis sur la présentation de la loi révisée à l'attention de différentes organisations représentatives.

Citons les formations assurées à l'INAP (Institut national d'administration publique) à l'Ecole de Police, les présentations et conférences assurées en collaboration avec l'Internet Society Luxembourg, la Fedil, la Chambre des Métiers, la Caisse de Maladie des Ouvriers, l'ABBL, le réseau intégré des gestionnaires de ressources humaines de l'administration publique (SIGEP), la « Employment Law Specialists Association » (ELSA) et le Clussil (Club de la Sécurité des Systèmes d'information, Luxembourg).

2.1.3 Demandes de renseignements

Le nombre de demandes de renseignements soumis en 2007 à la Commission nationale est resté à un niveau élevé mais stable, avec de nouveau quelque 1.900 demandes de renseignements par téléphone. Au total les demandes de renseignements se chiffrent pour 2007 à 2.018 contre 2.080 demandes enregistrées en 2006.

Une optimisation continue, tant sur le plan organisationnel qu'au niveau de la qualité des réponses données, permet cependant de traiter désormais les demandes plus rapidement (et certainement aussi de manière de plus en plus pointue).

2.2 Supervision de l'application de la loi

2.2.1 Formalités préalables

2.2.1.1 Généralités

Le nombre de notifications ordinaires a augmenté en 2007, traduisant ainsi une sensibilité plus élevée à se mettre en conformité (après l'adoption de la loi modificative) des acteurs susceptibles de notifier leurs traitements de données et un rythme de travail accru de la Commission nationale, grâce notamment à des formalités optimisées et simplifiées (nouveau formulaire).

Ainsi, le nombre traité de notifications ordinaires est passé de 250 en 2006 à 760 pour l'année 2007 tandis que celui de notifications simplifiées est passé de 890 en 2006 à 537 en 2007, avec comme total 1.297 dossiers de notification traités en 2007 contre 1.140 en 2006.

Les demandes d'autorisation préalable introduites en 2007 ont sensiblement augmenté par rapport à 2006, en passant de 314 à 543 dossiers au total.

Un certain tassement avait été observé en 2005 et 2006 traduisant l'attente d'un allègement de la procédure, notamment en matière de systèmes de surveillance. La publicité faite aux décisions judiciaires qui ont statué sur l'admissibilité comme preuve en justice d'images enregistrées par un dispositif de vidéosurveillance n'ayant pas été autorisé préalablement, ainsi que l'introduction d'un formulaire spécifique facilitant la demande d'une telle autorisation expliquent sans doute en partie l'accroissement du nombre de dossiers de ce type.

Même si la rapidité de l'examen des demandes d'autorisation a pu être optimisée, il faut souligner que les critères de légitimité et de proportionnalité, de caractère compatible avec la finalité initiale, la durée et les conditions de conservation des données prévues par la loi, doivent être appréciés au cas par cas, en fonction des circonstances et du contexte particulier de chaque demande. Ils rendent ainsi impossible une standardisation maximale dans l'examen des dossiers.

Il reste à statuer au sujet de l'autorisation de quelque 1.000 traitements de données pour lesquels la Commission nationale se trouve saisie d'une demande.

Le nombre total de dossiers de formalités préalables est passé de 1.454 en 2006 à 1.840 en 2007. Fin 2007 le nombre total de dossiers introduits depuis 2003 s'établit à 11.900, 3.754 déclarants / responsables avaient accompli des formalités contre 3.300 fin 2006.

2.2.1.2 Evolution récente au niveau des notifications et des demandes d'autorisation

Suite aux modifications par la loi du 27 juillet 2007, on peut noter une régression notable du nombre des notifications reçues depuis l'automne 2007.

Cette diminution s'explique par le fait que beaucoup de traitements « anodins » sont désormais exemptés de notification. Pour un grand nombre de petites et moyennes entreprises dont les formalités s'étaient limitées à l'introduction d'une notification simplifiée dans le passé, les modifications de la loi ont donc amené une simplification non négligeable des formalités administratives.

Un changement est intervenu également au niveau des traitements sur le crédit et la solvabilité des personnes. Les demandes d'autorisations introduites avant le 1er septembre 2007 par les professionnels du secteur financier qui en sont dispensés depuis lors ont fait l'objet d'une conversion en notification. Dans ce domaine, la Commission nationale n'aura probablement pas à s'attendre à un volume de notifications important, vu qu'une grande majorité des « PSF » présents au Luxembourg avaient déjà introduit une demande d'autorisation y relative avant la modification de la loi et n'auront dès lors plus à notifier leurs traitements.

Enfin, les traitements de catégories particulières de données (données sensibles) ayant fait l'objet d'une demande d'autorisation avant septembre 2007 ont également été enregistrés comme notifications suite aux modifications de la loi.

Ces traitements sont en cours d'inscription au registre public tenu par la Commission nationale et consultables en ligne sur son site Internet. Compte tenu des exemptions de l'obligation de notification introduites par la loi du 27 juillet 2007, le nombre devrait diminuer considérablement au cours des mois à venir.

Outre les simplifications légales, des mesures prises à l'initiative de la Commission nationale au cours de l'année sous revue ont permis d'accélérer le traitement des formalités préalables. Celle-ci a eu l'occasion de préciser les critères et d'arrêter les arbres de raisonnement qu'elle applique à l'égard des principaux types de traitements de données soumis à son autorisation. Cette standardisation plus poussée s'est accompagnée de mesures organisationnelles (nouveaux formulaires et modèles de décision, autorisations uniques) et d'un renforcement des effectifs avec effet au premier semestre 2008.

2.2.1.3 Les chargés de la protection des données

Au niveau de la désignation de chargés de la protection des données, on peut constater une très légère augmentation. Depuis septembre 2007 les organisations, entreprises, administrations, associations et institutions ont la possibilité de choisir une personne salariée comme chargé de la protection des données. Un nombre plus important d'entreprises devraient à l'avenir faire usage de cette faculté optionnelle pour les responsables de traitements. La contrainte du recours à une personne externe à l'entreprise et le coût afférent avaient fortement limité jusque-là le succès de la fonction de chargé de la protection des données qui reste facultative. Tandis que dans le passé la Commission nationale délivrait d'abord un agrément aux personnes intéressées de remplir cette fonction avant que ces dernières ne fassent l'objet d'une désignation, il est désormais d'usage que l'agrément soit délivré quasiment en parallèle avec la désignation d'une personne interne, désignation effectuée par le responsable du traitement.

2.2.1.4 Autorisation en cas de transferts de données vers des pays tiers

Dans le domaine des garanties appropriées nécessaires pour l'autorisation des transferts de données à caractère personnel vers des pays non membres de l'Union européenne n'assurant pas un niveau de protection adéquat, la Commission nationale a pu gagner en expérience et faire des progrès importants en 2007.

Une vingtaine de dossiers de ce type introduits par des sociétés et groupes d'entreprises souvent mondialement connus ont été examinés ou ont fait l'objet de décisions en 2007.

Parmi eux figurent aussi les chartes de règles contraignantes en matière de transferts internationaux de données de cinq grands groupes multinationaux. Ces chartes étaient également soumises pour approbation aux autorités de protection des données de plusieurs autres pays de l'Union européenne.

2.2.1.5 Approbation de règles contraignantes d'entreprises

En matière d'approbation de règles contraignantes d'entreprises (BCR – « binding corporate rules » sorte de formule alternative imaginée par le groupe dit « de l'article 29 » pour simplifier l'adoption de garanties appropriées pour les personnes concernées en cas de transfert de données à caractère personnel vers des pays tiers par un nombre important de sociétés d'un groupe, ceci rendrait compliqué le recours à un montage contractuel), la Commission nationale a dû se prononcer deux fois au courant de l'année 2007. Les BCR de deux grands groupes internationaux ont été approuvées par les délibérations respectives du 2 mars 2007 et du 6 juillet 2007. D'autre part, la Commission nationale a été impliquée pendant l'année 2007, et depuis mi-2006, dans trois autres procédures de coopération pour l'approbation de BCR n'ayant pas abouti à ce jour.

2.2.2 Plaintes et investigations

Le nombre de plaintes et demandes de vérification de licéité a connu une légère augmentation avec 34 dossiers en 2007 contre 30 en 2006.

Il est à relever que la Commission nationale a également voulu procéder à des actions d'investigation de sa propre initiative (sans qu'une question n'ait été portée à son attention), en se concentrant notamment sur les traitements de données d'envergure ou particulièrement sensibles (comme l'analyse à laquelle ont été soumises en 2005/2006 les mesures

organisationnelles internes et de sécurité des données pratiquées au Centre Commun de la Sécurité Sociale et de l'Assurance Maladie).

Une étude similaire est actuellement en cours dans le secteur des communications électroniques. A notre grande satisfaction, elle se déroule avec une collaboration aussi volontariste et constructive des responsables des entreprises concernées, à l'instar des organismes de la sécurité sociale.

Une importance particulière est attachée aux questions de sécurité des infrastructures et réseaux, de limitation des accès aux données, aux moyens d'empêcher et de constater des fraudes ou abus ainsi qu'à la responsabilisation du personnel.

Notons que dans ce dernier cas l'investigation avait débouché sur un plan d'action pluriannuel comprenant la mise en place ou le renforcement de diverses mesures susceptibles d'améliorer le niveau de protection et de sécurité des données et une responsabilisation accrue du personnel.

2.3 Information du public

2.3.1 Actions de sensibilisation du public

La Commission nationale a pris un certain nombre d'initiatives visant à sensibiliser le public le plus large aux enjeux de la protection des données à caractère personnel et de l'informer des règles applicables, notamment des droits reconnus aux personnes concernées par les traitements.

L'année 2007 a été aussi celle du lancement, à l'initiative du Conseil de l'Europe avec l'appui de la Commission européenne, de la « Journée européenne de la protection des données », journée qui s'est tenue pour la première fois le 28 janvier 2007 et qui sera dorénavant organisée chaque 28 janvier, journée anniversaire de l'ouverture à la signature de la « Convention 108 de Strasbourg ». La Commission nationale a participé à cette journée, notamment avec une campagne de communication comportant une annonce publiée dans la presse écrite et électronique ainsi qu'une communication avec les médias sous forme de dossier de presse, suivie par une série d'articles de presse et d'interviews de son président.

2.3.2 Reflets de l'activité de la Commission nationale dans la presse

Au total, on a cité la Commission nationale et le thème de la protection des données 143 fois dans la presse luxembourgeoise en 2007, contre 79 citations comptabilisées pour 2006.

Pour ce qui est des articles de presse dans leur entièreté, il y a lieu de relever deux grandes couvertures de la thématique de la protection des données à caractère personnel. Il s'agit tout d'abord d'un entretien avec le président de la Commission nationale paru dans l'édition d'avril (23.03.2007) du mensuel économique « PaperJam » (« Expliquer la loi, sensibiliser les citoyens »). L'autre grande couverture est le numéro spécial du périodique Forum « Aufgepasst Privatsphäre » n° 265, du mois d'avril 2007, consacré au thème de la surveillance. La protection des données y est abordée sous l'angle des libertés citoyennes ainsi que des risques d'une société de surveillance.

Parallèlement la Commission nationale, représentée par son président ou un autre membre effectif, est à plusieurs reprises intervenue directement dans les médias pour parler de différents sujets relatifs à la protection des données.

La panoplie des thèmes évoqués a été très vaste avec une large couverture de la Journée européenne de la protection des données (6 citations, respectivement articles de presse), la modification de la loi ainsi que les initiatives de simplification des formalités (16 citations), différents sujets d'actualité, tels le dossier SWIFT (11 citations), la vidéosurveillance sur les lieux publics (10 citations) et les limitations prévues dans ce domaine.

Outre la communication par voie de presse (un communiqué a été publié en juin 2007 pour annoncer les simplifications introduites dans la procédure d'autorisation et un autre pour rendre attentif à l'entrée en vigueur de la loi du 27 juillet 2007 et à l'impact des modifications intervenues), la présentation des enjeux de la protection des données fait régulièrement l'objet d'exposés et de conférences publiques, notamment dans certains lycées, à l'Université du Luxembourg, auprès d'organismes divers comme le CLUSSIL et la Luxembourg Internet Society.

2.3.3 Outil de communication : le site Internet

Le site Internet (www.cnpd.lu) représente le vecteur de communication courant pour la communication avec le public auquel la Commission nationale entend proposer :

- une information de base en la matière à l'attention des citoyens et du public en général, notamment à travers les rubriques « Actualités » et « Droits des personnes concernées » ;
- une documentation approfondie par thèmes (« Dossiers thématiques ») pour les lecteurs avertis, conseillers et responsables d'entreprise avec des liens facilitant des recherches sur les thèmes importants ;
- une plateforme interactive pour l'accomplissement en ligne des formalités prescrites par la loi, la consultation du registre public des traitements (« fichier des fichiers ») et les réactions des citoyens.

En effet, les formalités de notification peuvent être remplies quasiment « avec un clic » sur le site Internet de la Commission nationale.

Ainsi, en 2007, 37 % des notifications (simplifiées et ordinaires) ont été remplies en ligne par le biais du formulaire électronique.

C'est surtout un public averti qui a consulté le site Internet de la Commission nationale, ce qui se reflète dans les statistiques mensuelles de fréquentation.

La fréquentation révèle aussi l'intérêt des internautes aux travaux parlementaires de la révision de la loi de 2002, avec une hausse considérable de la fréquentation du site lors des débats parlementaires et un suivi sur les changements intervenus après l'entrée en vigueur de la loi.

Le site Internet de la Commission nationale a affiché au total 256.196 visites en 2007, ce qui correspond à une moyenne de 701 visites par jour (sur 365 jours), et allant jusqu'à 1.600 visites journalières. Ce sont les mois de juillet et de septembre 2007, avec respectivement quelque 35.000 et 32.000 visites contre une moyenne mensuelle de 21.349 visites qui ont enregistré les scores les plus importants.

Le site Internet constitue un moyen d'information important pour la Commission nationale qui a fait le choix d'utiliser cet outil de communication pour informer de manière permanente et continue sur les évolutions en matière de protection des données à caractère personnel et ce aussi bien sur le plan national qu'européen et international.

2.3.4 Formations et conférences

La Commission nationale saisit aussi régulièrement l'occasion d'expliquer les règles légales dans le cadre d'exposés ou de formations destinées à un public averti ou aux professionnels d'un secteur déterminé. De telles conférences ont été organisées en 2007 par l'ELSA (association d'avocats spécialisés en droit du travail), la Chambre des Métiers, les sociétés de sécurité Brinks et G4S, la FEDIL, l'ABBL, le réseau SIGEP des responsables des ressources humaines de la fonction publique, le CLUSSIL et les associations « Mensa » et la « Internet Society Luxembourg ».

Outre les formations et conférences précitées (notamment les formations assurées à l'Institut national de l'administration publique et à l'Ecole de Police), il y a lieu de relever l'intervention de la Commission nationale dans le cadre de la formation « Management de la Sécurité des Systèmes d'Information» (MSSI) à l'Université du Luxembourg.

La gestion de la sécurité des systèmes d'information devient une compétence critique pour la plupart des entreprises et des administrations. Dans le secteur financier par exemple, les nouveaux accords de Bâle imposent aux instituts financiers non seulement une gestion des risques financiers, mais aussi une gestion des risques opérationnels. Les systèmes d'information constituent certes un risque opérationnel majeur, mais ils fournissent parallèlement un potentiel de maîtrise des risques en mettant à disposition des outils automatiques pour améliorer le suivi des opérations.

Pour répondre à la demande d'une formation spécialisée, le Conseil de gouvernance de l'Université du Luxembourg a décidé de mettre en place un master professionnel en « Management de la Sécurité des Systèmes d'Information ».

La Commission nationale a participé activement à cette formation. Ses objectifs sont de sensibiliser les responsables de la sécurité des systèmes d'information à la problématique de la protection des données à caractère personnel (renseignements sur le site de l'Université du Luxembourg http://moodle.fdef.uni.lu/MSSI/).

2.4 Avis et recommandations

A la demande du gouvernement, la Commission nationale a émis sept avis en 2007 sur des projets de loi ou des dispositions réglementaires. Ces avis sont reproduits dans les annexes du présent rapport annuel ensemble avec d'autres prises de position et décisions adoptées par la Commission nationale de sa propre initiative.

2.4.1 Avis en matière de coopération interadministrative et d'échange de données au sein de l'administration étatique

Une illustration marquante de la position de la Commission nationale envers les échanges et partages de données relatives aux citoyens par l'administration publique se trouve dans l'avis du 23 mai 2007 portant sur l'avant-projet de loi ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des Contributions Directes, de l'Administration de l'Enregistrement et des Douanes et de l'Administration des Douanes et Accises et portant modification de différentes lois les concernant.

Selon les auteurs de l'avant-projet de loi, l'échange d'informations entre les différentes administrations a notamment comme finalités :

- l'établissement correct et le recouvrement des impôts, droits, taxes et cotisations ;
- la lutte contre l'évasion et la fraude fiscale ;
- la garantie du principe de l'égalité des citoyens et des entreprises devant l'impôt.

Dans le cadre des limites légales imposées en matière d'interconnexion, la Commission nationale a analysé si les données détenues par les différentes administrations sont bien traitées par d'autres administrations interconnectées aux premières de manière compatible avec les finalités pour lesquelles elles ont été collectées à l'origine. Suivant la doctrine, les finalités d'un traitement ultérieur sont réputées compatibles si la personne concernée a raisonnablement pu les prévoir.

Dans l'optique de rechercher un équilibre satisfaisant entre simplification administrative, efficacité et respect du droit à la vie privée dans la société de l'information, la Commission nationale a notamment préconisé :

- de prévoir une nomenclature précise des données échangées par les différents organismes publics en procédant à une énumération limitative par fichier public ;
- de prévoir des garanties spécifiques pour les catégories particulières de données visées aux articles 6 et 8 de la loi du 2 août 2002 ;
- de définir pour chaque type de coopération administrative la nature exacte de l'échange de données ;
- de prévoir des garanties au niveau de la confidentialité des données et de la sécurité des traitements au sens des articles 21, 22, 23 et 25 de la loi du 2 août 2002.

Dans des avis subséquents (notamment celui relatif au projet de loi n° 5802 sur la libre circulation des personnes et l'immigration adopté en début de l'année 2008), la Commission nationale a été amenée à appliquer le même raisonnement pour apprécier l'admissibilité de l'accès par une administration étatique aux données personnelles figurant dans les fichiers tenus par une autre administration.

2.4.2 Avis d'initiative relatif à l'interprétation et à l'application de l'art 28 de la loi du 21 septembre 2006 sur le bail à usage d'habitation et modifiant certaines dispositions du Code civil

Interrogée par la Ville de Luxembourg sur les aspects de protection des données à prendre en compte lors de l'établissement d'un cadastre des loyers, la Commission nationale a adopté lors de sa séance du

23 novembre 2007 un avis avec ses recommandations relatives à l'interprétation et à l'application de l'article 28 de la loi du 21 septembre 2006 sur le bail à usage d'habitation.

En rendant cet avis public, elle voulait fournir une guidance susceptible d'orienter non seulement les responsables de la Ville de Luxembourg mais aussi les responsables d'autres communes sur la façon la plus conforme à la législation sur la protection des données à caractère personnel de collecter et de traiter les données relatives aux loyers, locataires et bailleurs de logements destinés à l'habitation.

L'article 28 de la loi précitée autorise chaque commune « à demander annuellement auprès des bailleurs donnant en location un ou plusieurs logements sis sur le territoire de la commune, respectivement auprès des locataires d'un logement sis sur le territoire de la commune, des renseignements relatifs au montant du loyer et des charges locatives à payer au bailleur ainsi qu'au type et à la surface en m^2 du logement loué ».

L'alinéa 2 du même article précise que « ces renseignements peuvent être utilisés pour l'établissement d'un cadastre des loyers afin de connaître le niveau moyen des loyers demandés pour les différents types de logements dans une commune ou dans une partie de celle-ci ».

Si la loi sur le bail à usage d'habitation ne définit pas la notion de « cadastre des loyers », il résulte clairement des documents et débats parlementaires préalables à l'adoption de la loi sur le bail à usage d'habitation que le législateur entendait introduire une sorte de « Mietspiegel » tel qu'il existe en Allemagne.

La finalité de l'établissement du cadastre des loyers, en revanche, est définie par cette même loi comme la connaissance du niveau moyen et de l'évolution des loyers demandés pour les différents types de logements dans une commune ou dans une partie de celle-ci. Les objectifs du cadastre des loyers ainsi déterminés par le législateur se confondent avec ceux du « Mietspiegel » allemand.

La Commission nationale avait constaté lors de l'analyse comparative des législations allemande et luxembourgeoise qu'à la différence de l'établissement des « Mietspiegel » allemands l'enquête menée en vue de l'établissement du cadastre des loyers devait avoir un caractère exhaustif (du moins en théorie). Cette enquête était censée intégrer l'ensemble des logements loués sis sur le territoire d'une commune.

Si en Allemagne la collecte des données se fait moyennant des formulaires remplis soit sans référence à des données personnelles, soit avec indication de données personnelles mais rendues anonymes lors de leur saisie informatique, il faut constater que ni la loi sur le bail à usage d'habitation, ni un texte réglementaire ne contiennent des précisions quant à une méthodologie d'établissement du cadastre des loyers.

Or la Commission nationale a estimé d'une part que la collecte des données doit être limitée aux renseignements mentionnés à l'alinéa 1er de l'article 28, et d'autre part que le cadastre des loyers doit reposer sur un fichier anonyme, c'est-à-dire un fichier ne contenant aucune donnée à caractère personnel.

Enfin, l'anonymisation des données concorde avec la finalité légale du cadastre des loyers, purement statistique. Elle consiste à calculer périodiquement sur base de données effectives et fiables le niveau moyen des loyers pratiqués pour les différents types de logements dans une commune ou une partie de celle-ci et à rendre ces informations disponibles.

Le fichier ne devrait donc pas être établi en fonction des noms des propriétaires et/ou locataires ni en fonction de l'adresse de l'immeuble, mais il devrait être structuré suivant la typologie des logements retenue (nature, nombre des pièces, surface habitable, année de construction/rénovation, etc.) et suivant le quartier, respectivement la localité. Le souci d'anonymisation impose par ailleurs de renoncer à une différenciation par quartiers dans les petites communes.

En ce sens la Commission nationale a préconisé dans son avis que :

- les données à caractère personnel figurant sur les formulaires ne soient pas transcrites dans le fichier du cadastre des loyers lors de leur saisie informatique ;
- les formulaires et, le cas échéant, les listes d'adresses correspondantes soient détruites

dès que le niveau moyen des loyers pour les différents types de logements aura été déterminé ;

- les données du cadastre des loyers ne soient pas rapprochées ou mises en corrélation avec d'autres bases de données nominatives de la commune ou de tiers.

La Commission nationale a par ailleurs discuté avec les responsables du ministère du Logement et de l'Observatoire du Logement assuré pour ses besoins par le CEPS -INSTEAD les aspects de protection des données dont il convient de tenir compte dans la réalisation d'une étude relative au marché locatif et à l'évolution des loyers après l'entrée en vigueur de la loi sur le bail à usage locatif de 2006.

2.5 Participation aux travaux européens

Au courant de l'année 2007, la Commission nationale a continué à participer à différents groupes et sous-groupes de travail au niveau européen. Il s'agit notamment de « l'Internet Task Force » (ITF) qui constitue un sous-groupe du groupe de l'article 29 ainsi que du « groupe de Berlin », dédié à la protection des données privées dans le secteur des communications.

Ainsi, les représentants de la Commission nationale ont participé à une vingtaine de réunions sur le plan européen. Ces réunions, qui se démarquent souvent par un degré de technicité élevé, demandent généralement une préparation approfondie et un suivi continu des matières traitées.

Il s'agit de six séances du WP29 (Comité européen des Commissaires à la protection des données) institué par l'article 29 de la directive, des réunions des trois (sur une dizaine de) sous-groupes aux travaux desquelles participe un membre ou collaborateur de la Commission nationale (Internet et nouvelles technologies, données médicales, flux internationaux de données) du séminaire biannuel d'échanges d'expériences dans le traitement des cas pratiques («Case Handling Workshop »), de la réunion annuelle du Comité consultatif de la Convention 108 du Conseil de l'Europe (T-PD) et de la Conférence annuelle des Commissaires à la protection des données.

Par ailleurs, les membres de l'autorité de contrôle de l'article 17 participent en alternance aux réunions des autorités conjointes de contrôle d'Europol, du système d'information « Schengen » et des autorités douanières.

Le membre effectif de la Commission nationale, informaticien de formation, a participé aussi à deux colloques de spécialistes consacrés à des thèmes technologiques et relatifs aux secteurs des télécommunications.

La liste avec les références des avis et documents de travail adoptés en 2007 par le groupe de l'article 29 par les différents sous-groupes et autres Comités figure en annexe du présent rapport d'activités. Notons le degré d'actualité des observations relatives aux dossiers médicaux électroniques que beaucoup de pays s'apprêtent à mettre en place. Une importance particulière revient sans doute aussi aux orientations sur le concept de données à caractère personnel (WP136), de responsable (« data controler ») et de traitement de données (« automatic processing ») respectivement par le groupe de l'article 29 et le T-PD du Conseil de l'Europe.

2.5.1 Sous-groupes thématiques : le sous-groupe « Données médicales »

Durant l'année 2007, un membre effectif de la Commission nationale a participé à plusieurs réunions du sous-groupe « Données médicales », en vue d'élaborer un document de travail sur le traitement de données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques.

Suite à ces travaux, le groupe article 29 a adopté le document de travail en question. Son objectif est de fournir une guidance sur l'interprétation du cadre juridique de protection des données applicable aux systèmes de dossier médical électronique (DME) et d'énoncer certains principes généraux. Ce document vise également à définir les conditions en matière de protection des données préalablement nécessaires à l'institution d'un système de DME à l'échelle nationale ainsi que les garanties appropriées applicables. En formulant onze recommandations, il a vocation à contribuer ainsi à l'application uniforme des mesures nationales adoptées sur base de la directive 95/46/CE.

Le document a ensuite été soumis à une consultation publique dont le résultat a été analysé par le sous-groupe dit « Données médicales ».

2.5.2 Sous-groupes thématiques : le sous-groupe « Case Handling »

Aux mois d'avril et de novembre 2007, la Commission nationale a participé aux réunions du sous-groupe consacrées aux expériences dans le traitement de cas pratiques « Case Handling Workshop » qui ont eu lieu respectivement à Helsinki et à Lisbonne.

Lors de ces travaux, une large panoplie de sujets a été discutée. Il y a lieu de relever les thèmes et sujets suivants :

- vidéosurveillance ;
- données de santé : dossiers médicaux électroniques et données de santé excessives collectées par les compagnies d'assurances ;
- protection des données et accès aux documents publics : situation dans divers pays et situation dans l'administration des Communautés européennes ;
- marketing direct : spam et prospection politique par e-mail ;
- listes noires dans différents secteurs tels que télécom, location, assurances ;
- crédit et solvabilité : sociétés de renseignements commerciaux et d'information sur la solvabilité et l'utilisation ultérieure des données concernant le crédit et la solvabilité à des fins de profilage et de marketing ;
- biométrie ;
- collecte de données personnelles sur Internet.

2.5.3 Les groupes de travail sur des sujets technologiques

Ce groupe de travail a traité un large éventail de sujets et thèmes qui touchent de plus en plus la vie quotidienne des citoyens.

2.5.3.1 Moteurs de recherche et respect du droit à la vie privée

De nombreuses informations à des fins de statistiques et de marketing sont enregistrées par la plupart des moteurs de recherche : leurs archives contiennent notamment les requêtes des internautes, ainsi que l'heure de la visite, le type de navigateur utilisé, l'adresse IP de l'ordinateur, etc.

Pour parvenir à retracer les recherches d'une seule et même personne sur une longue période, plusieurs possibilités existent : si l'utilisateur dispose d'une adresse IP statique, il est très facile d'identifier ses différentes visites. L'adresse IP étant bel et bien une donnée personnelle qui doit être protégée en tant que telle, ceci entraîne une série de conséquences en particulier à propos de leur exploitation à des fins publicitaires, commerciales et autres.

Mais généralement les fournisseurs d'accès à l'internet utilisent des adresses IP dynamiques pour leurs abonnés, c'est-à-dire des adresses qui changent à chaque connexion. Dans ce cas-là, les moteurs de recherche ont recours aux cookies permanents : des petits mouchards installés sur les PC des utilisateurs avec un numéro d'identification fixe permettent de reconnaître chaque visiteur lorsqu'il se connecte sur le site. L'identification est par ailleurs encore plus simple lorsque les utilisateurs s'authentifient pour utiliser un des services des moteurs de recherche.

Les préoccupations soulevées par l'ITF au sujet des problèmes relatifs aux moteurs de recherche (identification des internautes, rétention des données, interaction avec le consommateur potentiel) ont été rassemblées et présentées dans un document remis au groupe de l'article 29.

2.5.3.2 Carte à puce sans contact contenant les titres de transport

La liberté de circuler anonymement constitue une de nos libertés fondamentales. Or les cartes à puces contenant un micro-processeur enregistrent des informations, y compris des données à caractère personnel.

La collecte et le traitement des données relatives aux déplacements des personnes, sous la forme de la date, de l'heure et du lieu de la validation du titre de transport via une borne de contrôle à l'entrée ou à

la sortie du réseau de transport, sont susceptibles de porter atteinte à la liberté de circuler anonymement et au droit à la vie privée lorsque ces données sont associées à un élément permettant d'identifier la personne concernée, en l'occurrence le numéro de la carte.

Dans le cadre de ce sujet « l'International Working Group on Data Protection in Telecommunications (IWGDPT) » a publié un document intitulé : Working Paper on E-Ticketing in Public Transport (http://www.datenschutz-berlin.de/attachments/335/e-ticket_en.pdf).

2.5.3.3 Sensor-based networks – Radio-Frequency Identification

Des petites puces à radiofréquence, appelées « tags RFID » (Radio Frequency Identification, c'est-à-dire balises émettrices d'un code d'identification électronique) et grosses comme une tête d'épingle, sont en train de conquérir le monde. Le nombre de domaines dans lesquels ces puces radio sont utilisées est en constante croissance.

Elles reprennent progressivement la place des étiquettes à code à barres placées sur les emballages des marchandises et des biens connus de tous les consommateurs.

Intégrées dans des étiquettes « intelligentes », les balises « RFID » sont utilisées pour reconnaître ou identifier, à plus ou moins grande distance et dans un minimum de temps, un objet, un animal ou une personne. Ces puces presque invisibles sont capables de lire et de stocker des informations sans nécessiter un contact physique, uniquement par transmission d'ondes radio. Une informatique omniprésente et envahissante pourra être encore plus réelle qu'elle ne l'est déjà.

La Commission nationale a publié sur son site www.cnpd.lu, en rubrique « dossiers thématiques », un document sur le RFID : (http://www.cnpd.lu/fr/dossiers/rfid/index.html).

2.5.3.4 Protection des données personnelles dans les réseaux sociaux virtuels

En effet, Facebook, et plus largement tous les réseaux sociaux sur Internet révèlent des nouveaux enjeux en termes de protection de la vie privée. Ils offrent des services innovants et généralement gratuits, souvent en contrepartie d'une utilisation commerciale des données personnelles. Une fois en ligne, les informations personnelles sont plus ou moins largement diffusées, indexées et analysées.

La vie quotidienne est de plus en plus empreinte des technologies de communications, interactions sociales ou tout simplement des conceptions de loisirs des citoyens.

S'y ajoute que les participants révèlent de plus en plus, de façon consciente ou non, de nombreuses données concernant les contacts, loisirs, livres et films préférés, opinions politiques, journaux intimes, photos etc. concernant leur propre personne ou même celles de personnes tierces.

Les risques et dangers aux droits de la personnalité pouvant résulter d'une telle utilisation des plateformes d'Internet et des services qu'elle propose sont d'ailleurs en grande partie méconnus ou même ignorés des internautes, pour la plupart des adolescents.

2.5.3.5 Télévision numérique et vie privée

L'évolution de la télévision a été marquée par une série de changements et de révolutions technologiques. La télévision fonctionne comme un flux et pendant longtemps le téléspectateur n'en a pas eu la maîtrise. La fourniture de programmes télévisés et autres services vidéo et audio en tant que signaux numériques par des réseaux de données à bande large change, de façon significative, les caractéristiques de la production, de la distribution et de la consommation de produits multimédia.

Elle entraîne la convergence des secteurs de la communication, de l'informatique et des médias de masse en un réseau unique et interactif. De même, elle entraîne l'introduction de nouveaux paradigmes de navigation, permettant un accès aux médias audio-visuels au moyen de nouveaux outils ou de services comme les moteurs de recherche vidéo, la distribution « peer-to-peer », etc. Finalement, elle permet potentiellement la collection et le traitement de données à caractère personnel, collectées de sources différentes, par exemple les services « multiple-play ».

Les conséquences importantes de cette révolution sont, d'une part l'introduction de nouveaux moyens de distribution des contenus multimédia numériques, comme la télévision interactive numérique, l'IPTV, la télévision basée sur le web, etc., d'autre part le remplacement du récepteur de télévision par câble traditionnel par un système interactif et intelligent. Dans ces systèmes, les utilisateurs peuvent télécharger un flux vidéo spécifique ou une chaîne de télévision sur demande, et ces systèmes peuvent directement interagir non seulement avec les contenus d'un programme télévisé, mais également avec tout autre sorte de contenus relatifs à la télévision.

L'« International Working Group on Data Protection in Telecommunications » (IWGDPT) a publié le document suivant à ce sujet : « Working Paper on Privacy Issues in the Distribution of Digital Media Content and Digital Television » (http://www.datenschutz-berlin.de/attachments/349/digit_en.pdf).

3 Les temps forts de 2007

Les travaux de la Commission nationale ont été marqués par un certain nombre de dossiers et de priorités, soit imposés par le contexte politique et/ou l'actualité, soit choisis par la Commission nationale en fonction de l'importance de la thématique par rapport aux principes de la protection des données à caractère personnel.

3.1 Révision de la loi du 2 août 2002

Le projet de loi n° 5554 déposé le 6 mars 2006 à la Chambre des Députés par Monsieur le Ministre des Communications a été examiné dans leurs avis respectifs par :

- la Chambre des Fonctionnaires et Employés publics (14 juillet 2006) ;
- la Chambre des Employés Privés (14 juillet 2006) ;
- la Chambre des Métiers (14 juillet 2006) ;
- la Chambre de Travail (29 septembre 2006) ;
- la Chambre de Commerce (29 septembre 2006) ;
- et le Conseil d'Etat (30 septembre 2007).

La Commission nationale avait donné son avis dès le 5 décembre 2005, avis qui était donc susceptible d'être pris en compte dans les avis précités.

La Commission nationale a encore été consultée avant les discussions parlementaires par le Ministère ainsi que par la commission parlementaire au sujet de certaines de ses recommandations qui n'avaient pas été commentées ou n'avaient pas été retenues par le Conseil d'Etat.

Ce dernier avait en effet marqué son opposition formelle à l'égard de la nouvelle procédure prévue initialement, suivant laquelle les demandes d'autorisation préalable qui n'auraient pas été accueillies par une décision de la Commission nationale endéans un délai de trois mois seraient censées avoir reçu l'autorisation implicite de cette dernière (son silence valant alors autorisation et non pas refus comme dans le droit commun de la procédure administrative), à moins qu'un délai supplémentaire n'ait été demandé par la Commission nationale pour poursuivre l'examen approfondi si le dossier lui apparaissait particulièrement délicat.

Le Président de la Commission nationale avait été invité à répondre aux questions des députés au cours de deux réunions de la commission parlementaire (les 19 avril et 8 mai 2007), en particulier au sujet des propositions d'amendements (Document parlementaire 5554/07).

La commission parlementaire a proposé l'insertion d'un article 14bis nouveau dans la loi, suivant lequel les traitements à des fins de surveillance sur le lieu de travail mis en œuvre par l'employeur ne seraient plus de façon générale soumis à l'autorisation préalable de la Commission nationale, mais seulement dans le cas où celle-ci en déciderait ainsi au vu des éléments de la notification du traitement de données ; la Commission nationale juge dans ce cas si ce traitement comporte des risques particuliers et susceptibles de porter atteinte aux droits et libertés des personnes concernées, notamment à leur vie privée.

L'objectif primaire de ce paragraphe nouveau à ajouter à l'article 14 de la loi était de rendre la procédure d'autorisation plus efficace, tout en permettant à la Commission nationale de réorienter ses moyens d'action vers des activités jugées prioritaires. Aux yeux du Conseil d'Etat, la démarche préconisée était, en revanche, inacceptable en ce qu'elle aurait été susceptible de conduire à des résultats retors et opérant un renversement de la présomption entourant le silence de l'Administration dans le cadre de l'application du droit administratif général.

Pour ne pas affaiblir les droits des personnes concernées à l'égard notamment de projets de traitement à des fins de surveillance, le Conseil d'Etat avait demandé de maintenir telles quelles les dispositions initiales du paragraphe 2 de l'article 14 de la loi de 2002 déterminant les informations devant figurer dans les demandes d'autorisation adressées à la Commission nationale et ainsi de modifier le texte de l'article 14 précité.

Face à cette opposition formelle, la Chambre des Députés et le Gouvernement étaient confrontés au choix de maintenir le schéma proposé contre l'opposition formelle du Conseil d'Etat ou d'adapter les changements proposés par cette haute institution.

Dans cette deuxième optique, la commission parlementaire avait suggéré une alternative qui consistait à ne

plus soumettre à l'autorisation préalable tous les traitements à des fins de surveillance (article 10 de la loi de 2002) ainsi que les traitements à des fins de surveillance sur les lieux de travail (ancien article 11 L-261-1 du Code du Travail) mais à conférer à la Commission nationale le droit de soumettre à son examen préalable détaillé parmi les traitements notifiés ceux pour lesquels elle estime qu'ils représentent un risque particulier pour les libertés et droits fondamentaux des personnes concernées, notamment en matière du respect de la vie privée. Cette proposition s'inspirait du droit communautaire, à savoir de la procédure applicable en matière de notification à la Commission européenne des fusions et concentrations.

L'idée suggérée par la commission parlementaire procédait d'un souci d'accélérer les procédures et de permettre à la Commission nationale de limiter son examen approfondi préalable aux dossiers les plus délicats et sensibles en lui déléguant le pouvoir de faire en quelque sorte un tri préliminaire dans cette matière qui couvre 90 % des demandes d'autorisation lui soumises.

Le Conseil d'Etat n'a cependant pas suivi la commission parlementaire sur ce point et a insisté afin que tout traitement de données à caractère personnel poursuivi à des fins de surveillance fasse l'objet d'un examen détaillé et d'une décision écrite de la Commission nationale.

La commission parlementaire s'est finalement inclinée. Elle a renoncé à ladite proposition alternative, tout en maintenant ses autres amendements qui ont d'ailleurs apporté diverses améliorations et clarifications dans le texte de loi finalement adopté par la Chambre des Députés le 12 juillet 2007 à une large majorité (52 voix pour et 8 abstentions). Lors des discussions en séance plénière, un consensus sur l'objectif de simplification des formalités et de clarification de la loi s'était dégagé.

3.2 Simplification et accélération de la prise en charge des formalités légales

Les travaux en vue de la simplification des formalités ont constitué un élément important du travail de la Commission nationale en 2007. Ses interventions se sont situées à deux niveaux, à savoir dans le cadre de la révision de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (Projet de loi 5554) et de sa propre initiative.

3.2.1 La simplification des formalités dans le cadre de la révision de la loi

La loi du 27 juillet 2007 portant modification notamment de celle du 2 août 2002 relative à la protection des personnes à l'égard des traitements de données à caractère personnel comporte bon nombre de clarifications ainsi que d'allègements et de simplifications des démarches administratives imposées aux responsables de fichiers et traitements.

Les propositions faites par la Commission nationale dans son avis du 5 décembre 2005 ou ultérieurement à l'attention du ministère ou de la commission parlementaire ont été très largement suivies. Seule reste à régler la question du rajout de critères de légitimation additionnels applicables aux traitements à des fins de surveillance sur le lieu de travail mis en œuvre par l'employeur. Comme ces dispositions qui faisaient l'objet de l'ancien article 11 de la loi du 2 août 2002 sont intégrées désormais au Code du travail (elles forment L.261-1 et L.261-2), le parlement n'a pas pu opérer dans le cadre du projet n° 5554 de modification au niveau de ces règles légales particulièrement importantes. La Commission nationale espère que ses suggestions seront examinées dans un avenir proche lors d'une réflexion sur un autre dossier parlementaire.

3.2.2 La simplification des formalités à la propre initiative de la Commission nationale

Au-delà de l'accompagnement des travaux parlementaires dans le cadre de la révision de la loi du 2 août 2002, la Commission est aussi intervenue à sa propre initiative pour simplifier les formalités.

Il y a lieu de relever quatre initiatives pour l'année 2007 :

- décision unique en matière de contrôle d'accès ;
- décision unique en matière de gestion de l'horaire mobile ;

- élaboration d'un formulaire spécifique pour les demandes d'autorisation en matière de vidéosurveillance ;
- amélioration et adaptation du formulaire de notification.

Ainsi, dès le 22 juin 2007, la Commission nationale a mis en ligne un nouveau formulaire structuré de façon à faciliter l'indication et l'analyse des renseignements nécessaires pour l'autorisation des systèmes de vidéosurveillance.

Elle a en outre adopté des autorisations uniques en matière de contrôle électronique des accès et de surveillance des heures de travail dans le cadre d'une organisation selon l'horaire mobile.

L'employeur qui respecte les restrictions et conditions retenues par la Commission nationale peut désormais bénéficier de l'autorisation préalable requise en remplissant un simple engagement formel de conformité à retourner à la Commission nationale, suivant un modèle téléchargeable sur le site Internet de la Commission nationale.

Avec l'entrée en vigueur des modifications apportées à la loi, le traitement des données sensibles (opinions politiques, convictions religieuses, appartenance syndicale et renseignements relatifs à la santé) n'est plus soumis à l'autorisation préalable, tout en n'étant licite que dans les seuls cas prévus aux articles 6 et 7 de la loi.

Ainsi les traitements des employeurs nécessaires dans le cadre de l'organisation, du déroulement des élections sociales et du fonctionnement des organes de représentation des salariés font désormais l'objet d'une notification unique (procédure simplifiée). Les employeurs qui doivent nécessairement recourir à ces traitements afin de respecter les dispositions afférentes du droit du travail n'ont plus qu'à notifier un engagement formel de conformité.

L'examen par la Commission nationale des demandes présentées par les responsables de traitements de données à caractère personnel qui restent soumis à une autorisation préalable a pu être également accéléré de façon significative par des mesures d'organisation interne.

Au cours de l'année 2007, près de 500 traitements ont été autorisés (souvent avec certaines restrictions ou conditions à observer dans la mise en œuvre) et le nombre de traitements de données figurant dans le registre public (consultable en ligne sur www.cnpd.lu) a approché les 9.000.

S'il n'y a dorénavant plus de retard dans la prise en charge des notifications, il faudra toutefois compter encore quelques mois avant de venir à bout de l'engorgement actuel au niveau des demandes d'autorisation (en particulier de l'autorisation de dispositifs de vidéosurveillance ou de surveillance sur le lieu du travail).

Le renforcement de ses ressources en personnel et les simplifications intervenues récemment, en même temps que l'expérience acquise désormais dans ce domaine, permettent néanmoins à la Commission nationale d'aborder l'année 2008 avec davantage d'optimisme.

3.3 Quelques sujets délicats et arbitrages ardus

En 2005 et 2006, la Commission nationale a autorisé un nombre non négligeable de traitements de données sensibles et relatives à la santé. Ces derniers, bien que très strictement encadrés par les dispositions limitatives des articles 6 et 7 de la loi, ne donnent plus lieu désormais à autorisation préalable. La Commission nationale conserve bien entendu, même après la modification de la loi, le droit d'investiguer et de se prononcer dans le cadre de son pouvoir de contrôle a posteriori.

Parmi les types de traitements de données à caractère personnel qui restent soumis à autorisation, les traitements à des fins de surveillance (article 10 de la loi) et les surveillances sur le lieu de travail mis en œuvre par l'employeur (article 11 de la loi et L.261-1 du Code du Travail) fournissent le plus grand nombre de demandes introduites, encore que le recours à des données biométriques tend lui aussi à générer de plus en plus d'appétits. Les délibérations tournent donc essentiellement autour de la mise en balance des intérêts en cause.

Pour le surplus, les questions d'interconnexion de fichiers et d'utilisation à des fins autres que celles

pour lesquelles les données personnelles furent initialement collectées sont les plus complexes et les plus délicates.

Dans ce dernier domaine les intérêts avancés répondent presque toujours aux critères de légitimation prévus par la loi ; mais c'est la question de la nécessité et de la proportionnalité aux finalités poursuivies qui donne lieu à discussion.

Aussi la Commission nationale s'efforce-t-elle de limiter, respectivement d'encadrer sérieusement la prolifération de bases de données biométriques et les accès et échanges de données entre les administrations publiques poursuivant des missions distinctes.

3.3.1 Biométrie

L'autorisation des dispositifs de reconnaissance par empreinte digitale avec stockage des données dans une base de données n'est en principe consentie que dans les hypothèses où la finalité correspond à un enjeu de sécurité majeur (consistant la plupart du temps dans la protection de l'intégrité physique de personnes exposées à des risques particuliers) et dépassant l'intérêt (notamment l'optimisation du fonctionnement) de l'organisme demandeur lui-même.

En revanche, des systèmes de contrôle d'accès par reconnaissance du contour de la main (données biométriques qui ne laissent pas de traces) peuvent être autorisés sans restriction au niveau du lieu et des modalités de stockage des gabarits (qui peuvent donc se trouver sur le système et le réseau informatique du demandeur).

De façon générale, la Commission nationale n'est pas convaincue de la nécessité de voir se répandre trop rapidement les systèmes d'identification/ d'authentification des personnes par leurs caractéristiques biométriques ; à plusieurs égards la fiabilité et la sécurité de tels systèmes ne sont pas totalement garantis. Le test grandeur nature déployé pendant quelques mois dans la gare de Mayence et portant sur la reconnaissance faciale de deux cent volontaires parmi les 23.000 voyageurs quotidiens utilisant les escalators et traversant l'enceinte de la gare a simplement permis de dégager un taux de fiabilité tout à fait insatisfaisant.

Malgré l'évolution technologique et la sophistication permanente des moyens (l'exposition organisée en 2006 à la Cité des Sciences à Paris en a donné un reflet vivant), il semble également que la reconnaissance de l'empreinte digitale puisse encore beaucoup trop facilement être déjouée par la fraude et que toutes les techniques biométriques utilisées connaissent encore à l'heure actuelle un certain taux d'erreurs (de faux positifs ou faux négatifs).

Une saine prudence apparaît donc être toujours de mise avant une généralisation précipitée du recours à ces technologies.

3.3.2 Echange et partage de données entre administrations publiques

Au cours de l'année 2007, la Commission nationale a émis cinq avis relatifs à des projets de loi prévoyant l'accès d'une administration étatique à certaines données personnelles contenues dans les fichiers d'autres départements ministériels, administrations ou organismes publics.

L'appréciation des critères de nécessité (des moyens alternatifs, moins invasifs, seraient-ils suffisants pour atteindre l'objectif recherché ?) et de proportionnalité revêt généralement un caractère très délicat, alors que l'intérêt public (besoin de connaître tous les renseignements pertinents et exacts) et la simplification administrative (amélioration de la rapidité et de l'efficacité des procédures avec allègement des démarches demandées aux citoyens et aux entreprises) plaident fortement contre les impératifs de limitation inhérents à la protection des données.

Souvent l'échange ou le partage de données relatives aux administrés sont réalisés au moyen d'une interconnexion de données à caractère personnel telle que visée à l'article 16 de la loi pour laquelle des conditions particulières s'appliquent, qu'elle soit d'ailleurs autorisée par un texte légal ou réglementaire ou par décision de la Commission nationale. Le Conseil d'Etat considère l'interconnexion comme une opération délicate par nature qui doit toujours être entourée d'un maximum de garanties (Avis du 30 janvier 2007 dans Doc. Parl. N° 5554.5, page 11).

Il s'agit dans la démarche de la Commission nationale de trouver le juste équilibre entre les besoins d'une administration publique rigoureuse, efficace et moderne et la nécessaire dissuasion de la généralisation du rapprochement des données des citoyens, quels que soient les fichiers ou/ et les intérêts publics pour lesquels elles ont été recueillies par les différents organismes publics et administrations.

Deux aspects retiennent particulièrement l'attention de la Commission nationale dans ses avis et décisions dans ce domaine : les objectifs poursuivis par le rapprochement des données et le caractère compatible des intérêts publics poursuivis de part et d'autre et la protection de la sécurité et de la confidentialité des données (et le cas échéant du secret professionnel) dont elles sont censées bénéficier.

L'expérience des dossiers examinés et en cours laisse la Commission nationale avec des sentiments mitigés. D'une part, une grande satisfaction d'être de plus en plus souvent consultés et impliqués dès les travaux préparatoires à un stade où ses réticences et recommandations peuvent encore être dûment prises en compte, d'autre part la difficulté ressentie à véhiculer le message d'autolimitation sur la voie de la facilité consistant à rendre accessibles tous azimuts l'ensemble des renseignements le cas échéant disponibles dans d'autres parties de l'administration étatique ou para-étatique (on confronte la Commission nationale régulièrement avec l'interrogation rituelle : « Wollen wir die Daten, oder müssen wir die Bürger laufen lassen ? »).

Outre la sensibilisation aux libertés individuelles et à la modération dans l'accumulation de données sur les citoyens, son rôle se cristallise dans la créativité avec laquelle elle arrivera à suggérer des solutions pragmatiques adaptées aux situations concrètes.

Dans ce paradigme, les solutions techniques et mesures de sécurité revêtent souvent une importance cruciale. La modernisation des ressources de l'informatique publique (Etat, Communes et sécurité sociale) et l'amélioration continue des standards de sécurité, la mise en place d'une politique de sensibilisation du personnel, de procédures et mécanismes de contrôle peuvent permettre une avancée significative sur ce plan. La Commission nationale attachera aussi une grande importance aux options notamment techniques qui seront envisagées dans le cadre de la réforme de la loi du 30 mars 1979 relative au répertoire général des personnes et au numéro d'identification national qui fait actuellement l'objet de travaux d'un groupe interministériel conduit par le ministère de la Fonction publique et de la Réforme administrative, le ministère de l'Intérieur, le ministère de la Justice, la CNSAE, etc.

3.3.3 Géolocalisation et autres enjeux technologiques

Parmi les technologies nouvelles qui connaissent un essor fulgurant et dont il faudra suivre attentivement les effets à long terme, ce sont celles des étiquettes de radio-identification d'objets « RFID » (voir aussi sous 2.5.3.) comprenant des puces à lecture sans contact et le traçage des déplacements, notamment par la géolocalisation ou la reconnaissance automatisée des immatriculations des voitures, qui menacent d'exposer progressivement les citoyens à une surveillance de plus en plus poussée.

Si le dernier cas de figure (la lecture et l'enregistrement automatisés des plaques d'immatriculation des véhicules à certains endroits du réseau routier) n'a pas encore fait son entrée au Grand-Duché, il suffit de suivre l'évolution en Allemagne et au Royaume-Uni pour mesurer l'étendue de la collecte et des utilisations légitimes ou illégitimes de ces renseignements relatifs aux déplacements des personnes.

La liberté des citoyens de se déplacer librement et anonymement sans être surveillés dans tous leurs mouvements va au-devant de plus en plus de restrictions.

L'augmentation du nombre de demandes d'autorisation pour des traitements à des fins de surveillance au moyen de la géolocalisation est elle aussi révélatrice du même phénomène, encore que la légitimité d'un suivi de sa flotte de véhicules par l'employeur/l'entreprise est mise en avant la plupart du temps, avec des arguments très plausibles tenant à l'organisation des flux de travail et à l'allocation des ressources, voire à la sécurité des personnes et des marchandises transportées.

La géolocalisation par l'employeur des véhicules utilisés par les salariés peut être ressentie par ces derniers comme très intrusive, et sa nécessité devra donc être justifiée suffisamment par référence aux cas d'ouverture légaux (critères de légitimation qui sont énumérés de façon limitative par l'article L.261-1 du Code du travail), notamment par un impératif de sûreté et de sécurité de l'employé lui-même, du véhicule ou des marchandises dont il a la charge.

Signalons à ce propos qu'après l'adoption de la loi du 27 juillet 2007 portant révision de la loi du 2 août 2002, il reste au législateur à se prononcer sur les propositions relatives à l'ancien article 11 de la loi du 2 août 2002 avancées dans son avis du 5 décembre 2005 relatif au projet de loi 5554 par la Commission nationale [1].

Les cas d'ouverture qu'elle a suggéré d'ajouter à l'article L.261-1 du Code du Travail recouvrent en effet des situations qui peuvent dans certaines circonstances (à condition de passer les tests de nécessité et proportionnalité) justifier un traitement de données de géolocalisation par l'employeur comme en témoigne la position de nos collègues français (recommandation adoptée le 27 avril 2006 par la CNIL) qui l'admet, lorsque ces données apparaissent nécessaire pour « assurer une meilleure allocation des moyens pour des prestations à accomplir en des lieux dispersés ; le suivi et la facturation d'une prestation ; le suivi de temps de travail, lorsque ce suivi ne peut être réalisé par d'autres moyens ».

Le dernier alinéa du point que la Commission nationale proposait d'ajouter à l'article énumérant les cas de surveillance sur le lieu de travail susceptibles d'être mis en œuvre par l'employeur permettrait à l'autorité luxembourgeoise d'aligner son raisonnement sur celui suivi en France dans l'appréciation de l'admissibilité d'une surveillance par géolocalisation, alors qu'elle ne peut actuellement fonder ses autorisations que sur les besoins de sécurité et santé des travailleurs et de protection des biens de l'entreprise, ainsi que le suivi du temps de travail dans certains cas.

L'approche de la Commission nationale est rigoureuse dans l'appréciation de la proportionnalité. Les autorisations délivrées entourent ces traitements de conditions et de garanties appropriées, notamment par l'interdiction de collecter certaines données relatives au respect de la législation sur la circulation routière, d'informer convenablement les employés concernés et d'assurer un accès et une conservation très illimitée aux informations issues de la surveillance.

Pour terminer le passage en revue des questions de technologie rencontrées dans les travaux de la Commission nationale en 2007, il y a lieu de relever l'analyse du projet e-go du Ministère des Transports. Dans ce dossier elle a pu se baser sur les travaux du groupe de Berlin, auxquels participe l'un des membres de la Commission nationale, groupe ayant récemment adopté un papier d'orientation (http://www.datenschutz-berlin.de/attachments/335/e-ticket_en.pdf) relatif aux enjeux et aux précautions auxquels il convient de faire attention dans le domaine de l' « e-ticketing ».

Les réflexions du groupe de spécialistes de la protection des données dans le domaine des technologies de l'information et de la communication traduisent une tendance à la multiplication des intrusions externes sous forme de notification spontanée par les logiciels (fonction « calling home ») et du traçage de l'utilisation des terminaux IT et de communication électronique qui s'opèrent de plus en plus souvent à l'insu de l'utilisateur (on parle d' « ubiquitious computing »).

D'un autre côté, les technologies modernes livrent aux utilisateurs des moyens de plus en plus performants afin de détecter et de combattre les abus et de les guider dans les pratiques respectueuses de la vie privée (« Privacy Enhancing Technologies » PET), que ce soit la cryptologie et la signature électronique (PKI),

1 cf. doc. parl. N°5554-6 page 10 : elle préconisait le rajout d'une condition de légitimité libellée comme suit :

f) … *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 …

les outils de reconnaissance des « pourriels » et des intrusions à travers le réseau ou par Internet.

La protection des données ne reconnaît pas seulement dans le développement technologique son effet de multiplication des risques, elle reconnait aussi son aspect positif et son potentiel à constituer des remèdes et sauvegardes.

3.4 L'affaire SWIFT

L'affaire « SWIFT » a été déclenchée par des révélations de la presse américaine en juin 2006 sur le fait que la CIA et le département du Trésor américain avaient surveillé pendant des années des millions de données transitant par le réseau de la société SWIFT.

Cette information a causé un vif émoi lors des débats du Parlement européen ; ce dernier a demandé l'avis des autorités de protection des données après avoir constaté que la société SWIFT, dont le centre opérationnel se trouve à La Hulpe près de Bruxelles, avait mis à disposition des autorités des Etats-Unis, depuis 2001, des informations sur les transactions financières de milliers de citoyens de l'Union européenne. Les institutions européennes avaient conclu à la probable irrégularité de la surveillance du réseau par les autorités américaines au regard des règles européennes de protection des données personnelles.

La Commission belge de protection de la vie privée (CPVP), chef de file des autorités de protection des données européennes du fait de l'établissement de SWIFT en Belgique, avait rendu à ce sujet le 26 septembre 2006 au Premier ministre belge un avis concluant à la violation, par SWIFT, des règles belges de protection des données personnelles. La CPVP avait considéré que SWIFT aurait dû contacter les autorités belges et européennes avant de s'exécuter.

Le dossier a donné lieu ensuite à un avis du groupe de l'article 29 le 22 novembre 2006, institué par l'article 29 de la directive européenne 95/46/CE du 24 octobre 1995 (à la base de la loi modifiée du 2 août 2002). Le groupe de l'article 29 est un organe consultatif indépendant auprès de la Commission européenne rassemblant les représentants de chaque autorité de protection des données des pays membre de l'Union européenne qui coordonne l'analyse de l'affaire par les autorités nationales.

Les discussions de la Commission européenne avec les autorités américaines ont finalement abouti le 28 juin 2007 à un échange de courrier relatif au respect de la protection des données.

Le ministère des Finances des Etats-Unis (« United States Treasury Department ») a ainsi pris les engagements suivants :

- les données ne seront utilisées qu'à des fins de contre-terrorisme, ce qui s'applique également lors du transfert à d'autres autorités ou vers d'autres pays ;
- le ministère identifiera et supprimera endéans les 5 ans de leur réception toute donnée qui n'est pas nécessaire pour des investigations en matière de contre-terrorisme ;
- un superviseur chargé par l'UE aura le droit de contrôler annuellement si le ministère tient ses engagements ;
- les engagements seront publiés dans le journal officiel de l'UE et dans le registre fédéral des Etats-Unis.

La société SWIFT elle-même s'est engagée à prendre différentes mesures afin de se conformer aux prescriptions européennes relatives à la protection des données. Ainsi, elle adhérera aux accords « Safe Harbor » (code de conduite relatif à la protection des données à respecter par les sociétés américaines qui s'y soumettent volontairement). De plus, elle procédera au cours des deux années à venir à un remaniement de son architecture de stockage de données par la création d'un second centre opérationnel en Suisse, lequel reprendra la fonction de sauvegarde actuellement assurée par le centre établi aux Etats-Unis. Les données relatives à des transactions bancaires intra-européennes seront à l'avenir stockées uniquement en Europe (le stockage doublé aux Etats-Unis sera donc arrêté à l'issue d'une phase de transition nécessaire pour réaliser la modification technique d'envergure).

Depuis le débat de l'affaire SWIFT, la Commission nationale a été en contact régulier avec l'Association

des Banques et Banquiers (ABBL) et l'ALMUS, l'Association des utilisateurs SWIFT au Luxembourg, avec notamment une entrevue d'ordre général en octobre 2006 à laquelle participaient en outre l'ABBL, l'ALMUS et une représentante de la direction générale de SWIFT.

Faisant suite à la recommandation exprimée par le groupe de l'article 29, la Commission nationale a pour sa part invité en 2007 les banques et autres établissements financiers luxembourgeois à améliorer l'information fournie à leurs clients et à les avertir en toute transparence de l'accès des autorités américaines à certaine données relatives aux transactions financières mondiales, donc également européennes. Sa recommandation fut d'ailleurs parfaitement suivie par l'ensemble des établissements de la place grâce à la collaboration active de l'ABBL et de l'ALMUS.

3.5 Autorisation de flux de données vers des pays tiers ne disposant pas d'un niveau de protection adéquat

En principe, les données à caractère personnel peuvent uniquement être transférées dans les pays de l'UE et dans les pays présentant un niveau de protection adéquat (article 18 de la loi modifiée du 2 août 2002).

Toutefois, la loi modifiée du 2 août 2002 prévoit dans son article 19 diverses dérogations à cette interdiction. Lorsqu'aucune de ces dérogations ne s'applique, l'autorisation préalable de la Commission nationale doit être sollicitée pour le transfert. Le responsable du traitement doit offrir des garanties suffisantes au regard de l'utilisation qui sera faite des données personnelles exportées par le destinataire établi dans un Etat tiers dont la législation n'assure pas une protection adéquate, ainsi que relativement à l'exercice des droits correspondants des personnes concernées.

Face au constat qu'au Luxembourg un nombre croissant de sociétés internationales, surtout actives dans le domaine du commerce électronique, se sont récemment implantées, la Commission nationale est intervenue en 2007 à plusieurs reprises pour analyser des demandes d'autorisation.

Une telle demande d'autorisation est nécessaire à chaque fois qu'une entreprise implantée au Luxembourg transfère des données à une autre entité implantée dans un pays tiers à l'Union européenne, indépendamment du fait qu'il s'agisse d'une entreprise tierce ou d'une entité du même groupe (p. ex. filiale ou maison-mère).

En principe, deux types de solutions sont possibles pour accorder une telle autorisation en cas de transfert de données dans des pays tiers : ou bien l'entreprise concernée adopte des « binding corporate rules », c'est-à-dire des dispositions contraignantes à l'intérieur d'un groupe d'entreprise imposant des standards de protection des données répondant aux critères communautaires, ou bien l'entreprise concernée procède par voie de clauses contractuelles la liant avec des entités implantées dans des pays tiers et répondant elles aussi aux standards européens et luxembourgeois.

Les types de données soumis à autorisation préalable sont, à titre d'exemple, les données relatives aux clients, les données relatives aux fournisseurs ou encore les données relatives aux ressources humaines (collaborateurs de l'entreprise).

En 2007, la Commission nationale a donné deux autorisations à des entreprises disposant de « binding corporate rules » et une dizaine d'autorisations à des entreprises disposant de clauses contractuelles appropriées avec les entreprises susceptibles de recevoir les données personnelles.

Il s'agit à chaque fois de dossiers demandant une analyse approfondie et une analyse pondérée et prudente de la part de la Commission nationale, en tenant compte aussi bien de la sensibilité des dossiers, de l'importance des acteurs que du nombre des personnes concernées.

3.6 L'identifiant unique (N° de matricule national)

Depuis juin 2006, un groupe interministériel auquel participent les ministères de la Fonction publique et de la Réforme administrative, de l'Intérieur, de la Justice ainsi que des Classes Moyennes, du Tourisme

et du Logement, le Centre informatique de l'Etat et le Centre Commun de la Sécurité Sociale a été chargé d'élaborer un projet de loi dans le but de réformer la loi du 30 mars 1979 ayant introduit le répertoire général des personnes et le numéro d'identification national à l'usage de l'administration publique luxembourgeoise.

Ce groupe de travail collabore étroitement avec la Commission nationale.

Au cours de deux réunions, la Commission nationale a exprimé ses préoccupations sur le fait que la loi de 1979 n'est plus appliquée de manière rigoureuse, et que le recours au numéro national est de plus en plus incontrôlé. Elle a demandé que les orientations pour l'introduction d'un nouvel identifiant national, davantage sécurisé que le matricule actuel qui fait ressortir la date de naissance et le sexe des personnes, soient arrêtées le plus rapidement possible. Elle a indiqué aux représentants des différents ministères en charge de la préparation d'un projet de loi afférent que le problème central est celui d'éviter que l'identifiant national puisse rendre possible des interconnexions ou accès illicites de données ou de fichiers. La Commission nationale a notamment fait état des expériences belges et autrichiennes en la matière, suite notamment à deux visites dans ces pays.

3.7 Règlement grand-ducal relatif à la vidéosurveillance des espaces publics (art. 17 de la loi de 2002)

Dans le cadre de l'article 17 de la loi du 2 août 2002, relatif aux traitements de données opérés par la police pour des raisons de sauvegarde de la sécurité publique et de constatations des infractions pénales, une autorité de contrôle spécifique appelée « Article 17 » est chargée de contrôler et de surveiller ces traitements de données.

Les traitements de données concernées sont :

- traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions pénales mis en œuvre par la Police Grand-Ducale, par l'Inspection Générale de la Police et par l'Administration des Douanes et Accises ;
- traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique ;
- traitements dans des domaines du droit pénal effectués en vertu de conventions internationales (p. ex. Convention de Schengen), d'accords intergouvernementaux ou dans le cadre de la coopération avec Interpol ;
- création et exploitation de systèmes de vidéo-surveillance des zones de sécurité (tout lieu déterminé par règlement grand-ducal et accessible au public qui, par sa nature, sa situation, sa configuration ou sa fréquentation présente un risque accru d'accomplissement d'infractions pénales).

En effet, la législation luxembourgeoise diffère de celles de nombreuses législations étrangères dans la mesure où la loi de 2002, donc le droit commun, reste applicable sauf dispositions spécifiques de droit national et international, notamment concernant l'espace Schengen et Europol. La supervision de la conformité des traitements de données opérés par la police pour des raisons de sauvegarde de la sécurité publique et de constatation des infractions pénales n'est pas opérée par la Commission nationale, mais par une autorité de contrôle spécifique. Cette autorité « Article 17 » est constituée de deux des trois membres de la Commission nationale et du délégué du procureur général qui la préside.

L'entrée en vigueur du règlement grand-ducal relatif à la vidéosurveillance dans un but de sécurité publique a été précédée par une concertation étroite avec la Commission nationale, laquelle n'a pas manqué d'émettre certaines réserves et surtout de formuler une série de recommandations remises au ministre de la Justice pour ce qui concerne les restrictions et garanties appropriées qu'il conviendrait de prévoir dans le texte du règlement grand-ducal ; ceci dans un but du juste équilibre entre la finalité de la sécurité publique et le maintien des droits fondamentaux et libertés des citoyens.

Elle a noté avec satisfaction qu'il a été tenu compte de l'essentiel de ses observations dans le libellé final du

règlement grand-ducal adopté par le gouvernement,

Avant la mise en œuvre, les membres de la Commission nationale ont eu l'occasion de sensibiliser les agents et collaborateurs de la police affectés à cette activité aux droits fondamentaux et la législation en matière de protection des données à caractère personnel. Une journée entière de leur formation y a été consacrée.

Enfin, l'autorité spécifique de l'article 17 de la loi a inspecté et vérifié des installations, notamment en ce qui concerne le respect des limitations imposées par le règlement grand-ducal en matière de règles de stockage et de l'effacement des images stockées.

Cette visite d'inspection et de vérification a eu lieu quelques jours après l'entrée en vigueur du règlement grand-ducal.

3.8 Le projet « e-go »

Le ministère des Transports ensemble avec son prestataire technique a contacté la Commission nationale pour recueillir son appréciation sur les questions de protection des données susceptibles de se poser dans la mise en œuvre du projet e-go qui doit être mis en place prochainement à l'échelle nationale.

Les cartes e-go à puces contenant un micro-processeur enregistrent des informations, y compris des données à caractère personnel relatives aux déplacements des personnes titulaires d'un abonnement prépayé ou d'une carte de privilèges (date, heure et lieu de la validation du titre de transport).

Dans un premier stade de mise en œuvre du projet, les données relatives aux déplacements ne seront pas relevées sur base nominative, de sorte qu'il reste du temps pour résoudre les problèmes étudiés.

S'inspirant des orientations arrêtées par le groupe de Berlin (cf. 2.5.3.2 ci-dessus) et des recommandations émises par la CNIL à l'égard de projets similaires déployés dans d'autres pays européens avec des titres de transport électroniques, la Commission nationale a fourni ses observations visant à éviter des abus avec les informations relatives aux déplacements des personnes.

4 Perspectives

4.1 Introduction : un sondage intéressant réalisé auprès du public et des entreprises

La Commission européenne a réalisé fin 2007 / début 2008 une enquête « Flash » Eurobaromètre sur la protection des données dans la perception des citoyens, respectivement des responsables d'entreprises. Elle nous livre non seulement un état des sentiments du public à travers l'Europe, mais aussi certaines informations intéressantes sur l'évolution des réponses enregistrées à travers ce sondage au Grand-Duché de Luxembourg en comparaison avec celui effectué fin 2003.

Ainsi les deux tiers des citoyens se disent toujours d'une certaine manière soucieux de la façon dont les renseignements les concernant sont traités par ceux qui les collectent et sont inquiets de laisser des données personnelles sur Internet.

Le taux des citoyens qui pensent que les gens ne sont guère sensibles aux questions de protection des données a connu au Luxembourg une régression spectaculaire, passant de 80 % en 2003 à 56 %. Ce taux s'établit toujours en moyenne à travers les 27 Etats membres à plus de 75 % comme en 2003, ce qui avait conduit les autorités de protection des données à placer une priorité importante dans le travail de sensibilisation et d'information du public. 76 % des citoyens pensent que leurs informations personnelles bénéficient d'un bon niveau de protection légal au Grand-Duché (3e meilleur score) contre seulement 48 % en moyenne européenne.

Les scores obtenus au Luxembourg au niveau de la connaissance des droits des personnes concernées sont en revanche moins bons : seulement 22 % des personnes interrogées connaissent tous les droits reconnus aux citoyens par la législation en vigueur. Le Luxembourg occupe la 22e place sur 27 Etats membres. En revanche, le droit de chacun d'être préalablement informé du traitement de ses données est connu de 55 % des personnes interrogées, contre seulement 23 % en 2003 (42 % score moyen européen).

Parmi les responsables d'entreprises, seulement 8 % des personnes interrogées au Grand-Duché se disent très bien informées sur les obligations légales (13 % en moyenne européenne), 48 % se disent assez bien familiarisées avec le cadre légal de la protection des données (56 % en moyenne européenne) et 40 % pas réellement au courant (contre moins de 30 % en moyenne européenne).

Ces résultats confirment l'importance du travail d'information auquel la Commission nationale a consacré de grands efforts les trois dernières années. La notoriété de celle-ci dans l'opinion publique en général est d'ailleurs en nette progression. 29 % des personnes interrogées ont entendu parler d'elle et connaissent sa mission, contre seulement 23 % en 2003.

Si ce bon chiffre dépasse le score moyen relevé à travers l'Europe, il est moins spectaculaire que celui de la proportion des personnes déclarant avoir déjà été en contact avec l'autorité de protection des données, où le Luxembourg recueille un score remarquable de 20 % (moyenne européenne 6 %, respectivement 13 % en 2003).

Les citoyens indiquent s'être mis en relation avec l'autorité de protection des données principalement pour se renseigner sur leurs droits et faire vérifier le respect de la loi dans une situation donnée, alors que les raisons citées par les responsables d'entreprises sont en premier lieu un besoin de guidance (60 %) et les formalités administratives (notifications 56 %).

Sur ce dernier point il est à relever que 55 % des responsables d'entreprises luxembourgeoises interrogés estiment que le cadre légal est trop strict et que certaines contraintes qu'ils subissent en la matière ne seraient pas nécessaires (en moyenne à travers l'Union européenne : 28 %). Le législateur était donc bien inspiré de simplifier la loi et d'alléger les formalités purement administratives pesant sur les entreprises.

Les membres de la Commission nationale se sentent plutôt confirmés dans la définition de leurs priorités stratégiques par les résultats de cette enquête Eurobaromètre et de l'évaluation des scores recensés au Luxembourg.

4.2 Quelles priorités pour les années à venir ?

La Commission nationale s'est fixée un certain nombre de priorités qui s'inscrivent dans la logique du travail déjà effectué et des objectifs atteints à ce jour.

En effet, la Commission nationale souhaite mettre en avant les points suivants pour les années à venir :

1) information du public, sensibilisation et explication des règles légales

2) guidance à fournir aux entreprises, organismes et administrations publics et promotion des bonnes pratiques

3) simplification et accélération du traitement des formalités administratives avec focalisation sur les traitements et situations comportant des risques notables

4) coopération avec les autorités et les professionnels dans la recherche des solutions praticables et publication de recommandations thématiques et sectorielles

5) contrôles ponctuels concentrés sur des cas graves et des investigations menées spontanément à titre préventif pour des fichiers importants et sensibles où la confiance du public dans certaines institutions exige que le respect de la loi soit parfaitement assuré.

A l'issue des cinq premières années, la Commission nationale a atteint son rythme de croisière, le renforcement en cours du nombre de ses collaborateurs permanents, l'expérience acquise par ses membres et les simplifications intervenues au niveau des formalités administratives prévues par la loi lui permettront mieux dorénavant de répondre aux attentes du public dans ses différentes missions.

Tout en résorbant dans les mois à venir le retard accumulé dans l'examen des demandes d'autorisation en souffrance, dorénavant elle devra pouvoir faire face de façon équilibrée à ses différentes missions en se dégageant progressivement d'une part disproportionnée prise jusqu'ici par sa fonction administrative et en consacrant davantage d'efforts à ses autres tâches au niveau de la supervision de l'application de la loi, de ses fonctions de consultation, recommandation et de coopération avec les acteurs et de sa disponibilité pour les demandes des citoyens.

Pour l'essentiel, les étapes qu'elle s'était fixées dans la feuille de route tracée dans son rapport d'activités relatif à l'année 2003 ont été franchies ou au moins abordées.

La Commission nationale espère que son propre sentiment d'avoir gagné en maturité au niveau de l'appréciation équilibrée des intérêts en cause et des réponses concrètes fournies sera partagé au jour le jour par ses interlocuteurs. En tous les cas est-elle consciente de l'importance de son rôle dans la préservation des libertés et droits fondamentaux des citoyens, notamment de la protection de la vie privée tout en ne voulant pas pour autant freiner le développement technologique, la compétitivité des entreprises (en particulier de celles qui emploient des collaborateurs au Luxembourg) et la modernisation de l'administration publique.

Dans le domaine de la protection des données, beaucoup de dossiers comportent aujourd'hui une dimension internationale ou mondiale (p.ex. SWIFT). La coopération européenne des commissaires à la protection des données joue donc un rôle essentiel, non seulement pour l'approfondissement des connaissances théoriques et le suivi de la jurisprudence, l'harmonisation de l'interprétation et de l'application des dispositions communautaires, mais aussi pour l'échange d'expériences et l'étude des phénomènes et technologies nouvelles et même pour l'investigation et l'analyse de dossiers à dimension transnationale (p.ex. : action commune dans le secteur de l'assurance maladie complémentaire).

L'internet offre toujours de nouvelles possibilités aux utilisateurs, possibilités apportant non seulement plein d'avantages pratiques, mais comportant aussi des risques nouveaux et importants. La facilité avec laquelle les jeunes se sont approprié cet outil place les parents et les autorités publiques devant des enjeux nouveaux pour la sécurité des mineurs et des données personnelles les concernant (cf. « virtual social networks » tel Facebook, etc.).

La Commission nationale recherchera plus encore que dans le passé le contact avec les écoles et les associations de jeunes pour aider à les sensibiliser sur les risques (la Commission nationale soutient le site Internet LUSI.LU et diverses autres initiatives dans ce domaine) et les informer des droits et règles légales susceptibles de les protéger.

La jurisprudence internationale des derniers mois témoigne, elle aussi, de l'actualité des questions de protection des données et de la volonté des citoyens de préserver ce droit qui se trouve ancré dorénavant dans la Charte des droits fondamentaux de l'Union européenne.

Citons l'arrêt C-275/06 du 29 janvier 2008 de la Cour de Justice des Communautés européennes (Promiscae c/ Telefonica) qui retient que la protection effective du droit d'auteur ne justifie pas une surveillance systématique des internautes et que des entorses au principe de confidentialité des données relatives au trafic et aux communications électroniques ne sont admissibles que si elles sont prévues par des dispositions expresses du droit national respectant le principe de proportionnalité dans une société démocratique (article 8 § 2 de la Convention européenne des droits de l'homme).

Dans trois décisions récentes, la Cour constitutionnelle fédérale de Karlsruhe a tenu elle aussi à renforcer les principes de la protection des données, d'abord en rejetant le relevé systématique des plaques minéralogiques des véhicules sur les autoroutes allemandes et leur utilisation à des fins autres que le système de péage automatisé des transports lourds dont l'infrastructure électronique est mise à contribution, puis en posant des limites très strictes aux mesures législatives de surveillance de l'usage des communications électroniques et de l'informatique pour les besoins de la lutte contre le terrorisme et la criminalité organisée.

L'arrêt du 27 février 2008 (B.v.R. 370/07 ; B.v.R 595/07) est d'autant plus remarquable qu'il constitue la création jurisprudentielle d'un droit fondamental nouveau « à la confidentialité de l'usage et à l'intégrité des systèmes informatiques » qui vient s'associer aux droits préexistants de la personnalité, notamment à celui « à l'autodétermination informationnelle » issu d'une création jurisprudentielle similaire de la même Cour en 1983. Quel beau cadeau pour le 30e anniversaire de la loi fédérale sur la protection des données personnelles que l'Allemagne fête en 2008 en même temps que la France commémore les 30 années de sa loi « Informatique et Libertés ».

Le débat qu'ont suscité récemment les pratiques de surveillance agressive de son personnel de la chaîne de supermarchés LIDL, révélées par le magazine « Stern », montre à quel point le législateur luxembourgeois était précurseur en introduisant l'ancien article 11 dans la loi du 2 août 2002 (devenu les articles L. 261-1 et L.261-2 du Code du Travail) et en jetant ainsi les bases d'une protection de la vie privée des salariés sur le lieu de travail dans le sillage de la jurisprudence de la Cour européenne des droits de l'homme. En confiant à la Commission nationale la mission non seulement de vérifier la légitimité des traitements à des fins de surveillance de son personnel envisagé par l'employeur, mais aussi d'en apprécier concrètement (en tenant compte de l'avis du Comité mixte, si l'entreprise en dispose) la nécessité et la proportionnalité, le législateur a entendu protéger les travailleurs au Luxembourg contre des pratiques excessives comme celles qui défraient aujourd'hui la chronique en RFA.

5 Ressources, structures et fonctionnement

5.1 Rapport de gestion relatif aux comptes de l'exercice 2007

L'activité de la Commission nationale au cours de l'année 2007 a été marquée par :

- les efforts déployés pour optimiser la prise en charge des formalités préalables (notifications et demandes d'autorisations) et accélérer la prise des décisions afférentes ;
- l'examen d'un nombre substantiel de demandes d'autorisation introduites ;
- la concertation avec nombre d'organismes publics au sujet de dossiers et projets justifiant des recommandations relatives aux traitements de données personnelles, et l'adoption d'une dizaine d'avis relatifs à des projets de loi ou règlements grand-ducaux ;
- l'accompagnement du projet de loi N°5554 portant révision de la loi du 2 août 2002 sur la protection des personnes à l'égard du traitement des données à caractère personnel ;
- les actions menées en vue de la sensibilisation du public et de la guidance des responsables de traitements, notamment à travers diverses séances d'information et la participation à la première journée européenne de la protection des données ;
- la maintenance et les mises à jour de notre site Internet www.cnpd.lu (hébergé auprès du CIE).

Dépenses de fonctionnement

Les loyers et charges locatives supportés pour les locaux provisoires de la Commission nationale (pris en location dans l'attente de son implantation dans le 1er bâtiment administratif à ériger par l'Etat à Belval-Ouest) ont atteint 85.500,00.- € et sont en ligne avec les prévisions.

Les effectifs en personnel de la Commission nationale se composaient en 2007, outre les trois membres effectifs, de deux fonctionnaires de la carrière moyenne (rédacteurs), d'un employé à durée indéterminée assurant le secrétariat et de trois employés juristes à durée déterminée affectés au service juridique et de la documentation.

Les trois auxiliaires temporaires (dont un informaticien) que l'établissement public s'est vu affecté par l'administration de l'emploi au cours de l'année 2007 ont eux aussi collaboré activement au fonctionnement administratif et technique de la Commission nationale.

Les charges de personnel permanent ont progressé de 25 % par rapport à l'exercice 2006, principalement du fait du renforcement des effectifs par deux juristes.

Un grand effort fut accompli au cours de l'exercice 2007 pour résorber le retard dans l'enregistrement des notifications reçues en application des articles 12 et 13 de la loi et pour accélérer le traitement des demandes d'autorisation dont il reste plusieurs centaines à examiner par la Commission nationale.

La simplification et la standardisation des opérations internes ensemble avec de nouveaux formulaires électroniques interactifs ont permis d'alléger la procédure, avant même que les simplifications prévues dans les dispositions de la loi du 27 juillet 2007 n'entrent en vigueur.

Le niveau des mesures de sécurité organisationnelle et technique qui représente un volet important des garanties appropriées pour la protection des données personnelles est vérifié dans chaque dossier d'autorisation préalable. Mais il a fait également l'objet des investigations dont la Commission a pris l'initiative depuis 2005, même en dehors des cas où elle se trouve saisie de plaintes et demandes de vérification.

Pour les audits et vérifications à effectuer à ce niveau, la Commission Nationale a eu recours à deux experts externes spécialisés dans les questions de sécurité informatique et de bonnes pratiques organisationnelles.

Parmi les dépenses d'honoraires et frais d'experts et prestataires externes figurent également les honoraires d'avocats et factures de la fiduciaire qui tient la comptabilité et établit le bilan de l'établissement public.

Le niveau de ces charges, certes important, est resté conforme aux prévisions.

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.

Comme prévu au budget, les dépenses d'information du public et de communication s'élèvent à 26.854,27 €, compte tenu en particulier 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 32.744,58 €.

Le total des frais de fonctionnement encourus par l'établissement public au cours de l'exercice 2007 s'élève à 1.100.986,45 €.

Investissements

Le 1er septembre 2007 sont entrées en vigueur des dispositions modificatives concernant la législation sur la protection des données. Ces modifications d'envergure réduisent et simplifient les démarches formelles à entreprendre par les responsables d'un traitement de données à caractère personnel et précisent certaines dispositions de la loi du 2 août 2002. La Commission nationale a procédé à différentes adaptations au niveau des formulaires, des applications internes et du registre public. Les dépenses d'investissement y relatifs s'élèvent à 40.319,00 €.

Recettes

Le montant des redevances perçues en application des articles 37 paragraphe (4) et 13 paragraphe (4) de la loi s'élève à 54.790,00 €. 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 14.123,88 €.

Résultat d'exploitation

Etant donné que la Commission nationale n'avait pas encore eu à supporter en 2005 de loyers et charges locatives, le montant de 96.600 € initialement prévu au budget des dépenses de cet exercice a été déduit de la dotation annuelle de 1.029.000 € dont la Commission nationale a bénéficié en 2007 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 donc à - 99.672,57 € au 31 décembre 2007.

5.2 Personnel et services mis en place

La procédure à suivre et le fonctionnement de la Commission nationale ont été formalisés par un règlement intérieur (adopté le 29 novembre 2002) et un schéma de notification (adopté le 26 février 2003 et actuellement en voie de modification pour tenir compte des récentes modifications légales). 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 N°22 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.

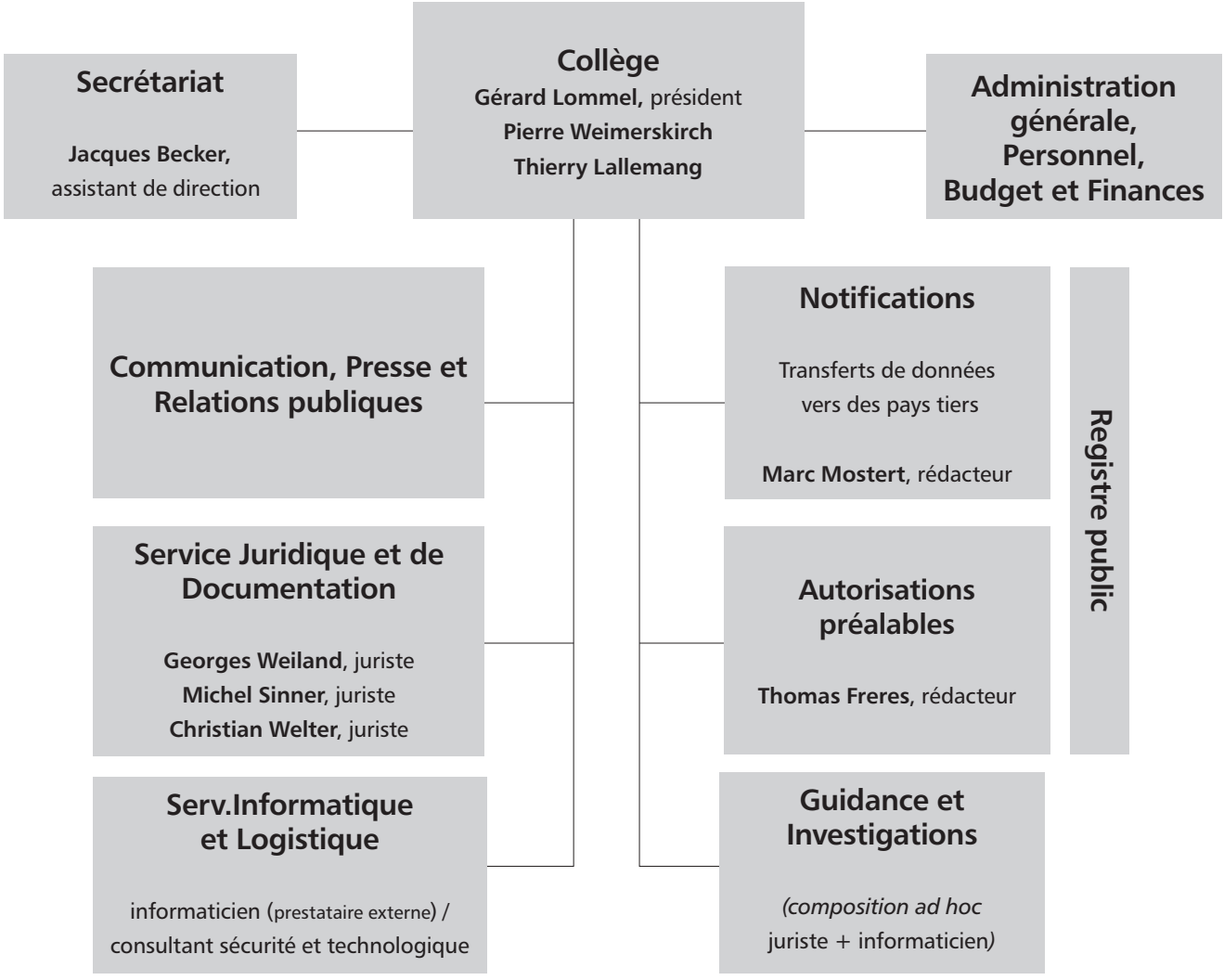
Les services de la Commission nationale ont été épaulés constamment par des auxiliaires mis à disposition par l'ADEM sous contrat CAT (nouvellement CAE) qui ont assuré différentes fonctions.

Membres effectifs	Gérard LOMMEL, président (juriste) Thierry LALLEMANG (juriste) Pierre WEIMERSKIRCH (informaticien)
Membres suppléants	Josiane PAULY (juriste) Véronique WAGENER (juriste), François THILL (informaticien)
Service juridique et de documentation	Georges WEILAND, juriste Michel SINNER, juriste Christian WELTER, juriste
Tenue du registre public et prise en charge administrative des notifications et demandes d'autorisations	Marc MOSTERT, rédacteur Thomas FRERES, rédacteur
Service informatique et de la logistique	
Administration générale et finances	Jacques BECKER, assistant de direction
Service presse et communication	

5.3 Bureaux

La Commission nationale occupe actuellement des bureaux provisoires à Luxembourg, 41 avenue de la Gare, au 4e étage, bureaux qu'elle occupe depuis l'époque où les locaux du 68, rue de Luxembourg à Esch-sur-Alzette se sont avérés trop exigus pour être partagés avec l'antenne régionale de l'Inspection du Travail et des Mines. Elle y conserve son siège officiel en attendant de revenir à Esch-sur-Alzette où il est prévu qu'elle emménage dans l'enceinte du « 1er Bâtiment administratif » de l'Etat, sur le site des friches industrielles de Belval-Ouest, bâtiment dont la construction prochaine s'inscrira dans le cadre de la politique de décentralisation des administrations publiques.

5.4 Organigramme



6 La Commission nationale en chiffres

• *Formalités préalables*

	2003	2004	2005	2006	2007	
a) Notifications						**TOTAL**
- notifications ordinaires	2.646	850	500	250	760	5.006
- notifications simplifiées	750	900	720	890	537	3.797
(Total a)	**3.396**	**1.750**	**1.220**	**1.140**	**1.297**	**8.803**
b) Autorisations préalables						
- demandes d'autorisation	765	406	317	295	392	2.175
- engagements de conformité	718	14	17	19	151	919
(Total b)	**1.483**	**420**	**334**	**314**	**543**	**3.094**
(Total général a) + b))	**4.879**	**2.170**	**1.554**	**1.454**	**1.840**	**11.897**
Déclarants (responsables ayant accompli des formalités)	2.220	2.500	2.850	3.300	3.754	

• *Demandes de renseignements*

	2004	2005	2006	2007
a) Demandes de renseignements par courrier				
- administrations publiques	18	7	8	6
- entreprises	49	10	8	5
- professions libérales	3	4	9	2
- citoyens	12	9	7	12
- associations	7	5	2	4
(Total a)	**89**	**35**	**34**	**29**
b) Demandes de renseignements par courriel				
(Total b)	**67**	**82**	**116**	**119**
c) Demandes de renseignements par téléphone				
(Total c)	**1.780**	**1.550**	**1.930**	**1.870**
(Total général a) + b) + c))	**1.936**	**1.667**	**2.080**	**2.018**

• *Plaintes et investigations*

	2003	2004	2005	2006	2007
- plaintes, demandes de vérification de licéité et investigations :	**15**	**38**	**40**	**30**	**34**

- *Séances de délibération*

	2004	2005	2006	2007
	39	36	39	40

- *Participations aux groupes de travail sur le plan européen*

	2004	2005	2006	2007
	28	33	23	22

- *Prises de contacts et concertations avec des organisations représentatives sectorielles ou acteurs*

	2004	2005	2006	2007
- secteur public	47	62	32	56
- secteur privé	30	38	12	40
(Total)	**77**	**100**	**44**	**96**

- *Séances d'information, conférences, exposés*

	2004	2005	2006	2007
	4	10	11	14

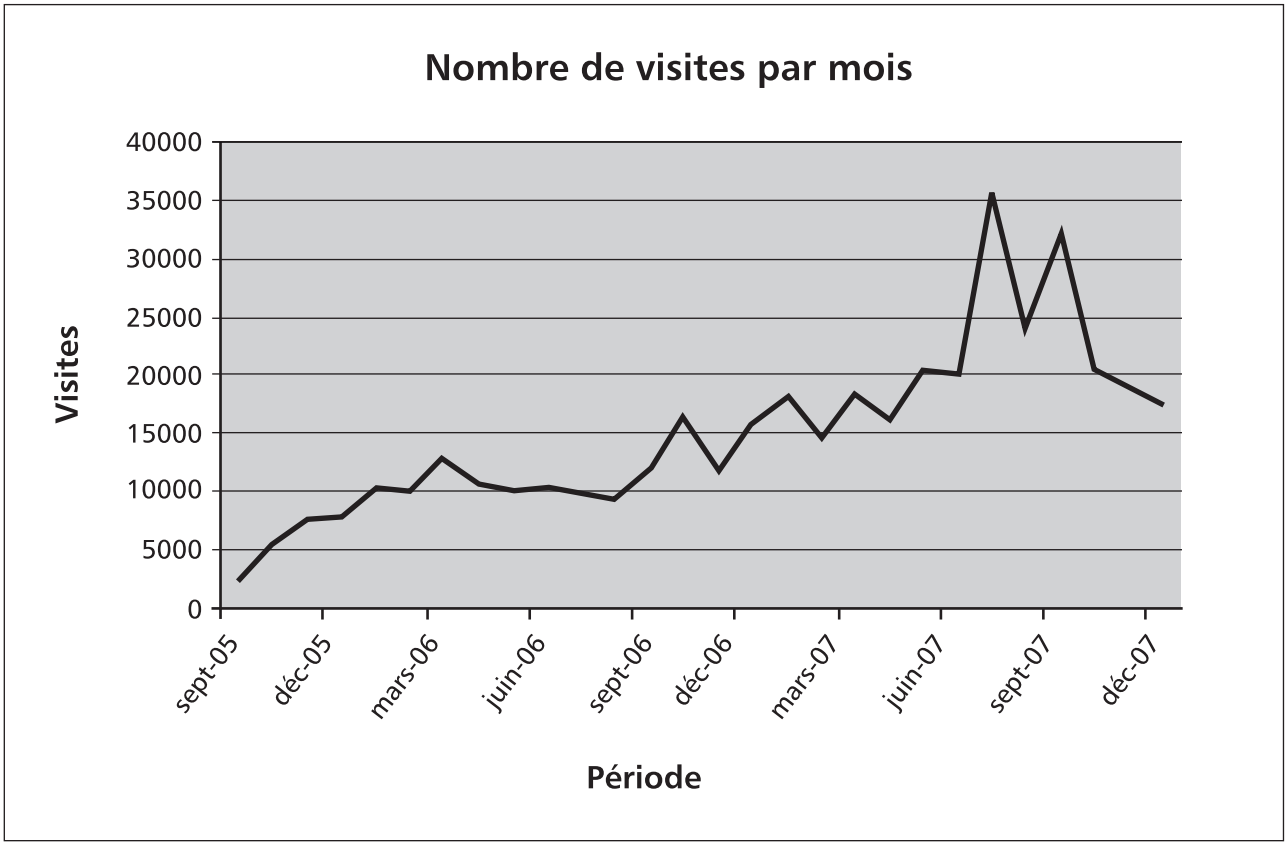
- *Campagne d'information du grand public*

2004	Brochures
2005	Relance du site Internet / Brochures version portugaise
2006	Calendrier ULC / Version anglaise du site Internet
2007	Campagne de sensibilisation dans le cadre de la 1re journée européenne de la protection des données

- *Reflets de l'activité de la Commission nationale dans la presse*

	2004	2005	2006	2007
Articles et interviews parus dans :				
- les quotidiens	14	16	67	127
- les hebdomadaires	5	6	4	9
- les mensuels	0	7	5	4
- les médias audiovisuels	1	3	3	3
(Total)	**20**	**32**	**79**	**143**

- *Fréquentation du site Internet*



ANNEXES

Avis et décisions

Avis de la Commission nationale pour la protection des données concernant l'avant-projet de loi ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des Contribution Directes, de l'Administration de l'Enregistrement et des Domaines et de l'Administration des Douanes et Accises et portant modification de différentes lois les concernant.

Délibération n°50/2007 du 23 mai 2007

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 des Communications en date du 21 mai 2007 que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet de l'avant-projet de loi prémentionné.

Celui-ci a pour objet d'instaurer une coopération interadministrative à trois niveaux, qui englobe neuf administrations différentes :

- l'échange d'informations – dans la mesure du possible de manière informatique – entre les deux administrations fiscales que sont l'Administration des Contributions directes et l'Administration de l'Enregistrement et des Domaines (Chapitre I de l'avant-projet de loi) ;
- l'échange de certaines données entre l'Administration de l'Enregistrement et des Domaines et l'Administration des Douanes et Accises et Inspection du Travail et des Mines (Chapitre II de l'avant-projet de loi) ;
- l'échange de données entre les deux administrations fiscales, d'une part, et l'Inspection Générale de la Sécurité Sociale et le Centre Commun de la Sécurité Sociale, d'autre part ; l'échange de données entre l'Administration des Contributions Directes, d'une part, et la Caisse Nationale des Prestations Familiales et le Fonds National de Solidarité, d'autre part ; la transmission d'informations relatives à la détention des véhicules automoteur par le Ministère des Transport aux deux administrations fiscales ainsi qu'à l'Administration des Douanes et Accises (Chapitre III de l'avant-projet de loi).

Selon les auteurs de l'avant-projet de loi, l'échange d'informations entre les différentes administrations a notamment comme finalités :

- l'établissement correct et le recouvrement des impôts, droits, taxes et cotisations ;
- la lutte contre l'évasion et la fraude fiscale ;
- la garantie du principe de l'égalité des citoyens et des entreprises devant l'impôt.

La Commission nationale pour la protection des données (ci-après « la Commission nationale ») voudrait relever d'emblée qu'elle comprend parfaitement la volonté du gouvernement de doter les administrations fiscales d'un système informatique moderne et performant, de permettre certains échanges de données et de favoriser une collaboration effective dans le cadre de la poursuite des finalités ci-avant mentionnées. Elle note par ailleurs que l'avant-projet de loi s'inscrit dans un contexte de simplification des procédures et de réduction des charges administratives des contribuables.

En revanche, le développement des échanges et partages d'informations entre les administrations publiques soulève par nature des interrogations quant à la préservation des libertés et droits fondamentaux, notamment la protection de la vie privée et des données personnelles. Dans l'exercice de sa mission de conseiller le gouvernement sur divers projets, la Commission nationale peut être amenée à exprimer des recommandations quant aux options les plus compatibles avec les principes de la protection des données personnelles.

Dans les développements qui suivent, la Commission nationale aborde les points les plus importants qui se dégagent de son examen de l'avant-projet de loi.

Bien que le texte de l'avant-projet de loi n'utilise pas le terme « interconnexion » tel qu'il est prévu aux articles 2 lettre (j) et 16 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), les auteurs de l'avant-projet de loi font expressément référence à l'article 16 de la loi du 2 août 2002 dans le commentaire de l'article 1.

Aux termes du paragraphe (3) de l'article 16, « *l'interconnexion n'est autorisée que dans le respect des finalités identiques ou liées…* ». Le législateur a en fait voulu renvoyer par cette disposition à la notion de compatibilité des finalités des traitements à interconnecter.

Se pose dès lors la question de savoir si les données détenues par les différentes administrations ne seront traitées par d'autres administrations interconnectées aux premières que de manière compatible avec les finalités pour lesquelles elles ont été collectées à l'origine. Suivant la doctrine, les finalités d'un traitement ultérieur sont réputées compatibles si la personne concernée a raisonnablement pu les prévoir.

Tout comme les auteurs de l'avant-projet de loi, la Commission nationale estime que tel sera généralement le cas en ce qui concerne le partage de données, moyennant interconnexion, entre l'Administration des Contributions Directes et l'Administration de l'Enregistrement et des Domaines, alors que chacune traite les données à des fins d'établissement et de perception des impôts, droits et taxes qui relèvent de sa propre compétence légale.

Ceci vaut également pour l'échange de données entre l'Administration de l'Enregistrement et des Domaines, d'une part, et l'Administration des Douanes et Accises, d'autre part, alors qu'il est limité à des aspects de perception de la TVA et de droits de douane à l'importation de biens en provenance de pays tiers non membres de l'Union européenne et se situe donc dans le cadre du même intérêt public.

Il en va cependant autrement en ce qui concerne l'échange de données entre les administrations fiscales et toutes les autres administrations dont les finalités primaires des traitements de données respectifs sont d'une toute autre nature que l'établissement, la perception et le recouvrement d'impôts, droits et taxes. En effet, au regard de l'article 16 de la loi du 2 août 2002, ces échanges de données posent, entre autres, le problème de la compatibilité entre les finalités découlant de la mission des administrations fiscales et de celles des autres administrations.

L'article 16 pose en ses paragraphes (2) et (3) un certain nombre de conditions supplémentaires auxquelles l'interconnexion doit répondre pour être licite :

- permettre d'atteindre des objectifs légaux présentant un intérêt légitime pour les responsables des traitements
- ne pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées
- être assortie de mesures de sécurité appropriées
- tenir compte du type de données faisant l'objet de l'interconnexion
- ne pas aboutir à vider de sa substance le secret professionnel auquel les responsables des traitements sont le cas échéant soumis,

Dans les cas où 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).

Or, à la lecture de l'avant-projet de loi, il y a lieu de constater que ce dernier se limite à instaurer le principe de l'interconnexion des données, respectivement de la coopération administrative à plusieurs niveaux par un échange de données, sans pour autant arrêter ou préciser les critères de délimitation, les conditions et les restrictions que devra respecter l'interconnexion de données envisagée.

La Commission nationale est cependant d'avis que l'avant-projet de loi sous examen devrait prévoir et fixer des critères et conditions au sens de l'article 16 de la loi du 2 août 2002. Ceci nous semble en particulier indispensable pour voir préciser la portée des articles 4, 7 et 8 de l'avant-projet de loi. Notons que le Conseil d'Etat, dans son avis du 30 janvier 2007 relatif au projet de loi n° 5554 portant modification de la loi du 2 août 2002, reste lui aussi « *convaincu que l'interconnexion de données constitue une opération délicate devant être entourée d'un maximum de garanties* ».

Les auteurs de l'avant-projet de loi laissent le soin au pouvoir réglementaire de déterminer les conditions, modalités et pratiques dans lesquels les échanges de données pourront avoir lieu.

Au stade actuel, la Commission nationale se trouve dès lors dans l'impossibilité d'apprécier dans le présent avis si les échanges de données envisagés dans l'avant-projet sont susceptibles de respecter à chaque fois la « ratio » des dispositions de l'article 16 de la loi du 2 août 2002.

En effet, plusieurs questions restent ouvertes :

Quels fichiers et catégories de données feront l'objet des échanges de données ?

Quelles sont les garanties en termes de confidentialité et sécurité des données ?

Les données protégées par un secret prévu par la loi seront-elles exclues ou bénéficieront-elles d'une protection particulière ?

Le législateur ne pourra mesurer toute la portée des interconnexions, ni vérifier leur proportionnalité, si le futur texte de loi n'intègre pas d'ores et déjà les conditions et garanties auxquelles elles devront répondre.

Il devra s'assurer du respect de l'article 8.2. de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales qui prévoit qu'il ne peut y avoir d'ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée que pour autant que cette ingérence est prévue par la loi et constitue une mesure qui, dans une société démocratique, est nécessaire à la défense d'un certain nombre d'intérêts publics légitimes.

Il aura à cœur d'éviter d'autoriser la mise en place successive d'interconnexions généralisées de fichiers publics, aussi importantes et nobles les finalités soient-elles. Il faut en effet garder à l'esprit qu'à la fin des années soixante-dix, l'adoption des législations européennes de protection des données procédait notamment de la volonté de protéger le citoyen contre des projets consistant à interconnecter l'ensemble des fichiers publics.

Il convient donc de rechercher un équilibre satisfaisant entre simplification administrative, efficacité et respect du droit à la vie privée dans la société de l'information.

En ce sens, la Commission nationale préconise notamment :

1. de prévoir une nomenclature précise des données échangées par les différents organismes publics 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 ;

2. de prévoir des garanties spécifiques pour les catégories particulières de données visées aux articles 6 et 8 de la loi du 2 août 2002 ;

3. de définir pour chaque type de coopération administrative la nature exacte de l'échange de données (p.ex. fichiers communs moyennant interconnexion entre deux ou plusieurs administrations ou communication « one way » par transmission, le cas échéant, systématique, sur demande ou spontanée) ; il faut en effet garder à l'esprit que dans l'optique de responsabilisation empruntée par la loi du 2 août 2002, les différentes administrations ne seront plus « maîtres » de leurs fichiers, dans la mesure

où d'autres organismes auront accès aux données ;

4. de prévoir des garanties au niveau de la confidentialité des données et de la sécurité des traitements au sens des articles 21, 22, 23 et 25 de la loi du 2 août 2002.

La Commission nationale est bien entendu disposée à conseiller le gouvernement sur ces points, notamment au niveau de l'élaboration des spécifications textuelles.

Enfin la Commission nationale voudrait relever qu'un groupe de travail interministériel est actuellement en train de préparer la réforme de la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales et le répertoire général des personnes.

Une importance cruciale reviendra aux mesures et garanties que le futur projet de loi prévoira dans l'intérêt de la protection des données personnelles et pour éviter des consultations et interconnexions abusives des données contenues dans les fichiers publics organisés par référence au numéro d'identité national.

Ces garanties comprendront prévisiblement aussi des mesures techniques et architectures sécurisées dont l'administration publique se dotera pour renforcer la confiance des citoyens dans l'administration électronique (par exemple mécanismes des « banques carrefour » en Belgique ou du numéro hautement sécurisé de la « Bürgerkarte » autrichienne).

En fonction des choix qui seront opérés les interconnexions licites, comme celles prévues dans l'avant-projet de loi sous examen, gagneront autant en terme de sécurité et confidentialité des données.

Avis de la Commission nationale pour la protection des données concernant un amendement à l'article 8 du projet de loi N° 5757 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des Contribution Directes, de l'Administration de l'Enregistrement et des Domaines et de l'Administration des Douanes et Accises et portant modification de différentes lois les concernant.

Délibération n°227/2007 du 16 novembre 2007

Conformément à l'article 32, paragraphe 3, lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après « la loi du 2 août 2002 ») et faisant suite à la demande lui adressée par Monsieur le Ministre des Finances en date du 8 novembre 2007, la Commission nationale pour la protection des données (ci-après « la Commission nationale ») a adopté lors de sa séance du 16 novembre 2007 un avis avec ses recommandations relatifs à l'amendement au projet de loi prémentionné.

La Commission nationale relève qu'elle a eu l'occasion en date du 23 mai 2007 de donner son avis relatif à l'avant-projet de loi et qu'elle a été suivie dans ses recommandations par les auteurs du projet de loi N° 5757.

Elle analyse dès lors l'amendement à l'aune des recommandations déjà avancées dans cet avis afin d'entourer d'un maximum de précautions et de garanties les échanges de renseignements à caractère personnel instaurés par ce texte.

Elle y constatait notamment que le projet de loi instaure des échanges de données moyennant interconnexion entre les deux administrations fiscales, à savoir l'Administration des Contributions Directes (ci-après « ACD ») et l'Administration de l'Enregistrement et des Domaines (ci-après « AED ») et certaines autres administrations. S'appuyant sur les travaux parlementaires[2], elle a par ailleurs considéré que l'élaboration de textes légaux ou réglementaires autorisant une interconnexion de données devrait respecter la ratio des dispositions de l'article 16 de la loi du 2 août 2002.

Ce dernier prévoit entre autres que « *l'interconnexion des données doit permettre d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements* ». La Commission nationale observe que la motivation de l'amendement fait ressortir un intérêt légitime consistant notamment à apprécier l'opportunité d'une assignation en faillite. Le partage des données entre les trois administrations concernées répond au souci de permettre à ces créanciers publics importants d'avoir une vue globale de la situation économique et financière des entreprises débitrices et de disposer de toutes les informations nécessaires pour prendre leurs décisions en connaissance de cause en matière de recouvrement de créances. Cet échange d'informations vise à permettre de recouvrir les créances en temps utiles dans l'intérêt de la collectivité et d'éviter des assignations en faillite inutiles d'entreprises financièrement saines, mais connaissant des problèmes de liquidités temporaires.

S'il est dès lors établi que l'intérêt des trois administrations en question est légitime et que leurs finalités respectives sont compatibles entre elles, il n'en reste pas moins nécessaire d'assortir l'interconnexion à autoriser par des mesures de sécurité appropriées.

En vue de respecter la ratio des dispositions de l'article 16 de la loi modifiée du 2 août 2002, le texte de l'amendement sous examen devrait prévoir et fixer les conditions et garanties au sens de cet article 16.

Dans cette optique et par analogie aux libellés d'autres dispositions du projet de loi, la Commission nationale estime que le texte de l'amendement devrait en premier lieu préciser davantage par quels moyens ont

2 doc. parl. N° 4735/13, p. 30

lieu les échanges d'informations, c'est-à-dire à l'aide de procédés automatisés ou non, et que les procédés automatisés se font moyennant interconnexion des données et sous garantie d'un accès sécurisé, limité et contrôlé.

Notons que le libellé actuel du texte de l'amendement ne comporte pas de précisions quant aux personnes concernées par le partage des données. Il faut donc en déduire que sont concernées par l'échange de données, l'ensemble des personnes physiques et morales susceptibles d'être assignées en faillite, sans distinction aucune entre des entreprises économiquement saines et de celles dont la situation financière est compromise. Il est vrai que la motivation de l'amendement fait référence à une « *transmission réciproque et ciblée de renseignements relatifs à l'endettement de certaines entreprises connaissant de sérieuses difficultés financières* ».

Il nous semblerait donc préférable que le texte précise que l'échange se limite aux données relatives aux arriérés concernant les seuls commerçants et sociétés commerciales dont la situation financière est compromise. Pour éviter que l'échange des données à caractère personnel ne prenne des proportions excessives, le texte devrait garantir qu'il porte uniquement sur un nombre limité de commerçants et de sociétés commerciales dont il y a réellement lieu de s'inquiéter de leur solvabilité, de sorte à exclure la majorité des entreprises financièrement saines.

Enfin, dans le même ordre d'idées, la Commission nationale est d'avis que la nature exacte des dettes respectives des débiteurs envers les administrations en question ne devrait pas être communiquée et que les informations échangées soient limitées au montant total des sommes exigibles. En effet, même si une concertation semble nécessaire, il paraît excessif, au regard des règles de protection des données, que le CCSS, par exemple, ait connaissance de la nature exacte de la dette qu'une entreprise « X » a envers une administration fiscale, ceci d'autant plus que les finalités découlant des missions des administrations respectives correspondent à des intérêts publics différents. Par ailleurs, les renseignements échangés ne devraient concerner qu'une période limitée, suffisante pour distinguer une situation financière définitivement compromise d'un problème de liquidités temporaires. Des spécifications textuelles s'imposeraient dès lors en ce sens.

Avis de la Commission nationale pour la protection des données relatif à l'interprétation et l'application de l'article 28 de la loi du 21 septembre 2006 sur le bail à usage d'habitation et modifiant certaines dispositions du Code civil.

Délibération n°228/2007 du 23 novembre 2007

Interrogée par la Ville de Luxembourg quant aux aspects de protection des données à prendre en compte lors de l'établissement d'un cadastre des loyers, la Commission nationale pour la protection des données (ci-après « la Commission nationale ») a adopté lors de sa séance du 23 novembre 2007 un avis avec ses recommandations relatives à l'interprétation et à l'application de l'article 28 de la loi du 21 septembre 2006 sur le bail à usage d'habitation.

L'article 28 de la loi précitée autorise chaque commune « *à demander annuellement auprès des bailleurs, donnant en location un ou plusieurs logements sis sur le territoire de la commune, respectivement auprès des locataires d'un logement sis sur le territoire de la commune, des renseignements relatifs au montant du loyer et des charges locatives à payer au bailleur ainsi qu'au type et à la surface en m2 du logement loué* ».

L'alinéa 2 du même article précise que « *ces renseignements peuvent être utilisés pour l'établissement d'un cadastre des loyers afin de connaître le niveau moyen des loyers demandés pour les différents types de logements dans une commune ou dans une partie de celle-ci* ».

La notion « cadastre des loyers »

La loi sur le bail à usage d'habitation laisse aux communes la faculté d'établir un cadastre des loyers à partir des données recueillies, via formulaires, auprès des bailleurs, respectivement des locataires.

Elle ne définit pas la notion de « cadastre des loyers ». Il résulte cependant clairement des documents et débats parlementaires préalables à l'adoption de la loi sur le bail à usage d'habitation que le législateur entendait introduire une « sorte de « Mietspiegel tel qu'il existe en Allemagne »[3].

Finalité du cadastre des loyers

Si la loi ne définit donc pas expressément la notion de « cadastre des loyers », elle précise cependant la finalité de l'établissement de celui-ci, à savoir la connaissance du niveau moyen et de l'évolution des loyers demandés pour les différents types de logements dans une commune ou dans une partie de celle-ci. Les objectifs du cadastre des loyers ainsi déterminés par le législateur se confondent avec ceux du « Mietspiegel » allemand[4].

La constitution et l'élaboration du cadastre des loyers

Ayant passé en revue la documentation qu'elle a pu trouver sur les modalités suivies en la matière dans certaines villes de la République fédérale d'Allemagne et analysé le fonctionnement pratique du « Mietspiegel », la Commission nationale constate qu'il n'existe pas en Allemagne de textes légaux ou réglementaires homogènes, ni au niveau fédéral, ni au niveau des « Länder », sur la méthodologie relative à la collecte des données en vue de l'établissement du « Mietspiegel ». La pratique diverge certes sur quelques points de détail d'une commune à l'autre ou d'un « Land » à l'autre. Il est cependant constant que le niveau moyen des loyers est déterminé à partir des résultats obtenus grâce à des enquêtes menées régulièrement auprès d'un échantillon représentatif des habitants d'une commune. Ces enquêtes sont réalisées moyennant formulaires à remplir par les habitants ou par des entretiens téléphoniques ; en tout état de cause la participation est facultative.

Au Luxembourg, le niveau moyen des loyers pour les différents types de logements dans une commune est

3 cf. doc. parl. 5216/00, p. 30

4 „Ein Mietspiegel ist eine Übersicht über die ortsübliche Vergleichsmiete"(§ 558c BGB), im frei finanzierten Wohnungsbau

censé être déterminé sur base des données relatives au montant du loyer et des charges locatives ainsi qu'au type et à la surface en m2 du logement loué. Ces données sont collectées par le biais de formulaires, soumis pour être complétés par les bailleurs, respectivement les locataires, qui sont obligés de les remplir et de les retourner à la commune sous peine d'amende (art. 28 alinéa 3).

A la différence de l'établissement des « Mietspiegel » allemands, l'enquête menée en vue de l'établissement du cadastre des loyers aura donc un caractère exhaustif (du moins en théorie), alors qu'elle est censée intégrer l'ensemble des logements loués sis sur le territoire d'une commune. Notons que l'article 558 du Code civil allemand (BGB) précise certaines conditions qui font présumer que le « Mietspiegel » reflète correctement les loyers pratiqués dans les localités pour lesquels il a été établi.

Contenu du cadastre des loyers et considérations en matière de protection des données et de la vie privée

En Allemagne la collecte des données devant servir à l'établissement du « Mietspiegel » se fait moyennant des formulaires qui sont remplis soit sans référence à des données personnelles, soit avec indication de données personnelles. Dans le dernier cas cependant, les données sont rendues anonymes lors de leur saisie informatique. Les formulaires et, le cas échéant, les listes des noms et adresses correspondantes de l'échantillon représentatif sont détruites une fois le « Mietspiegel » établi.

Ainsi, le chargé de la protection des données du « Land Berlin » relève au sujet du « Mietspiegel » dans son rapport annuel de 1997 : „*Unsere Hinweise zur Gestaltung der Erhebungsbögen bei den Mietern als auch zur Anonymisierung der Einzelangaben wurden berücksichtigt, so daß der Datenbestand in seiner anonymisierten Form als Grundlage für künftige Mietspiegel mit genutzt werden kann. (...) Eine personen-, wohnungs- oder adreßbezogene Nutzung sowohl der Daten des Statistischen Landesamt als auch des Mietspiegels ist durch die Anonymisierungsmaßnahmen ... ausgeschlossen worden*".

Ni la loi sur le bail à usage d'habitation, ni un texte réglementaire, ne contiennent des précisions quant à une méthodologie d'établissement du cadastre des loyers. Rappelons que la volonté du législateur était de prévoir une possibilité pour les communes d'établir un cadastre des loyers à l'instar du modèle allemand du « Mietspiegel ».

En tenant compte des observations qui précèdent et en considération de règles relatives à la protection des données et de la vie privée, la Commission nationale estime d'une part que la collecte des données doit être limitée aux renseignements mentionnés à l'alinéa 1er de l'article 28 (cf. en annexe : modèle de formulaire approuvé pour la Ville de Luxembourg), et d'autre part que le cadastre des loyers doit reposer sur un fichier anonyme, c'est-à-dire un ficher ne contenant aucune donnée à caractère personnel.

Cette question de l'anonymisation a également été soulevée par le Conseil d'Etat qui soulignait dans son avis[5] relatif au projet de loi sur le bail à usage d'habitation « qu'en tout état de cause les données visées devraient être anonymisées ».

Enfin, l'anonymisation des données concorde d'ailleurs avec la finalité légale du cadastre des loyers qui est purement statistique et consiste à calculer sur base de données effectives et fiables périodiquement le niveau moyen des loyers pratiqués pour les différents types de logements dans une commune ou une partie de celle-ci et rendre ces informations disponibles.

Le fichier ne devra donc pas être établi en fonction des noms des propriétaires et/ou locataires ni de l'adresse de l'immeuble, mais devra être structuré suivant la typologie des logements retenue (nature, nombre des pièces, surface habitable, année de construction/rénovation etc.) et suivant le quartier respectivement la localité. Le souci d'anonymisation impose par ailleurs de renoncer à une différenciation par quartiers dans les petites communes.

Il convient en effet de rechercher un équilibre satisfaisant entre l'intérêt légitime poursuivi par les autorités publiques et le respect du droit à la vie privée et des données personnelles des citoyens.

5 cf. doc. parl 5216/08, p. 9

En ce sens la Commission nationale préconise que :

- les données à caractère personnel figurant sur les formulaires, à savoir les noms, prénoms et adresses des bailleurs, respectivement locataires ne doivent pas être transcrites dans le fichier du cadastre des loyers lors de leur saisie informatique ;
- les formulaires et, le cas échéant, les listes d'adresses correspondantes doivent être détruites dès que le niveau moyen des loyers pour les différents types de logements aura été déterminé ;
- les données du cadastre des loyers ne doivent pas être rapprochées ou mises en corrélation avec d'autres bases de données nominatives de la commune ou de tiers ;
- elles ne doivent être publiées et diffusées que sous la forme de données chiffrées agrégées (fourchettes et moyennes) reflétant les loyers pratiqués en relation avec l'époque, la localité, le cas échéant le quartier et en fonction des caractéristiques (abstraites) du logement ;
- une différenciation par quartiers ne devra avoir lieu que dans les communes dépassant un certain nombre d'habitants de façon à ne pas rendre illusoire l'anonymat recherché.

Avis de la Commission nationale pour la protection des données concernant le projet de règlement grand-ducal portant création et exploitation d'un traitement d'informations de police générale (POLIS).

Délibération n°230/2007 du 23 novembre 2007

Conformément à l'article 32 paragraphe 3 lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée « la loi du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission d'« 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 de la Justice en date du 6 novembre 2007 que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de règlement grand-ducal prémentionné.

La Commission nationale a pris connaissance de l'avis du Conseil d'Etat du 23 octobre 2007 référencé n°47.240 et relatif au projet sous examen.

Remarques préliminaires

Le règlement grand-ducal sous examen vise un traitement qui conformément à l'article 17 paragraphe (1) de la loi du 2 août 2002, doit être autorisé par voie règlementaire.

Le règlement sous examen fait partie des traitements prescrits par son point (a) c'est-à-dire « *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 règlementaires respectives, aux organes du corps de police grand-ducale, de l'Inspection générale de la police et de l'administration des douanes et accises* ».

L'alinéa deuxième de l'article 17 paragraphe (1) lettre (a) de la loi du 2 août 2002 énumère un certain nombre d'indications que le règlement grand-ducal autorisant les traitements de données devra contenir.

La Commission nationale constate à ce propos que l'intégralité des indications requises y figurent de manière claire, explicite et circonstanciée, exceptions faites toutefois pour la condition de légitimité du traitement ainsi que pour l'origine des données traitées.

La Commission nationale propose de clarifier ces deux questions en intégrant dans le règlement grand-ducal sous examen la précision selon laquelle la condition de légitimité du traitement POLIS repose sur l'article 5 lettre (b) de la loi du 2 août 2002 à savoir sur la nécessité « *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 ou les tiers auxquels les données sont communiquées* ».

A titre liminaire, la Commission nationale relève encore que le traitement en question sera soumis au contrôle de l'autorité de contrôle instituée par l'article 17 paragraphe (2) de la loi du 2 août 2002 (ci-après : l'autorité de contrôle *ad hoc*). Cet article indique encore qu'un règlement grand-ducal précisera les modalités liées à l'organisation et au fonctionnement de ladite autorité. Cependant, aucun règlement grand-ducal n'a pour le moment été pris à ces fins.

Ci-après nous passons en revue les indications du projet de règlement grand-ducal correspondant aux exigences du paragraphe premier lettre (a) deuxième alinéa de l'article 17 de la loi.

1. Le responsable du traitement (article 1er du règlement)

Le règlement sous examen prévoit que le directeur général de la police grand-ducale est responsable unique du traitement.

2. Les personnes concernées par le traitement (articles 2 et 8 du règlement)

La Commission nationale relève que la liste des personnes concernées par le traitement est détaillée et

exhaustive. Elle fait sienne les observations et réserves formulées par le Conseil d'Etat dans son avis du 27 octobre 2007 précité. Dans un souci de respect de la protection de la vie privée, il est nécessaire que les catégories de personnes concernées soient davantage délimitées. En l'état actuel de l'article 2 du règlement sous examen, la Commission nationale estime que tout individu serait susceptible de figurer dans le traitement POLIS, que ce soit en qualité de victime, d'auteur d'une infraction ou de tiers.

3. Les catégories de données (articles 4, 5, 8, 9 et 14)

La Commission nationale note que le règlement grand-ducal sous examen reconnaît le caractère particulièrement sensible des données biométriques. Elle se satisfait que cette catégorie de données bénéficie d'un régime aménagé.

Tout en se ralliant aux observations formulées par le Conseil d'Etat dans son avis précité, la Commission nationale préconise d'apporter des précisions complémentaires à l'article 5 du règlement sous examen.

L'article 4 paragraphe (1) de la loi du 2 août 2002 détermine les qualités que doivent recueillir les données d'un traitement. Il en résulte en substance que les données doivent nécessairement revêtir un degré certain de précision.

Or, la Commission nationale estime que l'article 5 paragraphe (1) points 9, 11 et 12 ainsi que l'article 5 paragraphe (3) points 1 et 2 du règlement sous examen ne répondent à l'exigence de précision requise par l'article 4 paragraphe (1) de la loi du 2 août 2002.

4. Les destinataires (article 17)

L'article 17 comporte une énumération des destinataires dans des termes très généraux, qui risquent toutefois de ne contribuer que très imparfaitement à l'objectif de transparence recherchée.

En ce qui concerne le contenu la Commission nationale préférerait, à l'instar du Conseil d'Etat, que seules les parties «recherche» et «documentaire» du traitement POLIS soient susceptibles de faire l'objet d'une transmission.

Elle est encore d'avis qu'il ne faudrait pas autoriser l'accès à toutes les données, dans les limites de ce qui est techniquement possible. En effet, seules les données nécessaires à l'exécution des missions des destinataires doivent pouvoir être communiquées. A titre d'exemple, les données biométriques intéressent un nombre limité de personnes ou d'organismes ; compte tenu de la nature sensible de ces données, il est préférable que leur communication soit la plus encadrée possible. De plus, au vu de la nature sensible et particulière des informations contenues dans le traitement envisagé, il serait souhaitable qu'un nombre restreint de personnes puissent y accéder. La Commission nationale propose donc de préciser dans le texte que « *conformément aux règles de l'art et dans les limites de ce qui est techniquement réalisable, seules les données nécessaires à l'exécution des missions du destinataire peuvent être communiquées* ».

5. Les mesures de sécurité (article 18)

Les mesures de sécurité sont une obligation légale inscrite aux articles 22 et 23 de la loi du 2 août 2002. Elles permettent notamment d'assurer la fiabilité du traitement. Dans la mesure où l'article 23 premier paragraphe de la loi précitée prévoit déjà que les mesures de sécurité doivent être prises « *en fonction du risque d'atteinte à la vie privée ainsi que de l'état de l'art et des coûts liés à leur mise en œuvre* », le deuxième paragraphe de l'article 18 est superfétatoire, et ce d'autant plus qu'à première lecture, il semblerait que ces mesures puissent ne pas être prises.

La Commission nationale propose donc de supprimer le second paragraphe de l'article 18 du dit règlement et, le cas échéant, d'insérer une disposition qui renvoie aux dispositions inscrites à l'article 23 paragraphe 1er de la loi du 2 août 2002.

6. L'accès aux données (articles 4, 6 et 14)

Le règlement grand-ducal sous examen prévoit que la partie «recherche» du traitement POLIS sera accessible à tous les officiers et agents de police judiciaire, soit environ 1.500 personnes selon le rapport d'activités de la police pour l'année 2006. En outre, et conformément à l'article 16 du projet de règlement, l'administration des douanes aura accès à l'ensemble des données.

La Commission nationale se demande si cet accès n'est pas trop large et donc susceptible de faciliter des abus.

Toutefois, la Commission nationale est rassurée que, dans le souci de contrer d'éventuels abus, tout traitement d'informations de la banque de données fait l'objet d'une journalisation détaillée (les indications relatives aux informations consultées, aux dates et heures de la consultation, à la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation sont enregistrées). Ces conditions sont indispensables à l'exercice, par l'autorité de contrôle *ad hoc*, des missions de contrôle et de surveillance lui dévolues au titre de l'article 17 de la loi modifiée du 2 août 2002.

Afin d'être complet, ne conviendrait-il pas de prévoir que les membres de l'administration des douanes et accises ainsi que de l'Inspection générale de la police, qui accèdent au traitement POLIS, procèdent également à la journalisation détaillée conformément à l'article 4 ?

7. La durée de conservation (articles 7, 8, 11 à 14)

Bien que la durée de conservation des données ne constitue pas une mention obligatoire exigée par l'article 17 de la loi du 2 août 2002, le projet de règlement grand-ducal comprend des indications y afférentes. Par référence à l'article 4 paragraphe (1) de ladite loi qui veut que les données personnelles ne soient conservées qu'aussi longtemps que nécessaire, la Commission nationale relève que la conservation pendant une durée limitée est une garantie supplémentaire des libertés et droits des personnes concernées.

8. Les finalités du traitement (articles 1er et 14)

Conformément à l'article premier du projet de règlement sous examen, les finalités du traitement de données POLIS sont la prévention, la recherche et la constatation des infractions pénales. Toutefois le volet archivage du traitement POLIS est établi à des fins différentes de contrôle interne, de statistiques et de recherche historique.

9. Les droits des personnes concernées

Les articles 27 paragraphe (1) lettre (d) et 29 paragraphe (1) lettre (d) de la loi du 2 août 2002 instituent des exceptions au droit à l'information et au droit d'accès des personnes aux données les concernant lorsque le traitement a trait, comme dans le traitement envisagé dans le règlement grand-ducal sous examen, à la prévention, la recherche, la constatation et la poursuites d'infractions pénales.

Ainsi le droit à l'information n'est pas applicable en l'espèce ; le droit d'accès des personnes concernées subsiste mais il peut être limité et différé. La Commission nationale suggère de compléter le projet de règlement grand-ducal en précisant dans quelles mesures le droit d'accès est limité et différé en la matière. Dans ce cas, il est indirect et l'article 17 paragraphe (2) dernier alinéa précise qu'il est exercé par le truchement de l'autorité de contrôle *ad hoc* qui procède aux vérifications et investigations et qui informera la personne concernée de la conformité légale du traitement en question.

Avis de la Commission nationale pour la protection des données concernant le Chapitre 5, article 7 du projet de loi N° 5801 portant introduction du boni pour enfant et modification de différentes lois.

Délibération n°240/2007 du 30 novembre 2007

Conformément à l'article 32, paragraphe 3, lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après « la loi du 2 août 2002 ») et faisant suite à la demande lui adressée par Monsieur le Ministre des Finances en date du 7 novembre 2007, la Commission nationale pour la protection des données (ci-après « la Commission nationale ») a adopté lors de sa séance du 30 novembre 2007 un avis avec ses recommandations relatifs à l'article 7 du projet de loi prémentionné.

Le projet de loi en question apporte des modifications importantes à certaines dispositions législatives en matière d'impôts sur le revenu et d'allocations familiales. Il a surtout comme objet de changer la façon dont il est tenu compte de la charge que représentent les enfants et de remanier fondamentalement le système de la modération d'impôt pour enfants. L'introduction d'un boni pour enfants est censée favoriser les familles avec des enfants à charge et touchant des revenus faibles et moyens. Tous les enfants en bénéficient, y compris ceux des contribuables ne payant pas d'impôts.

En vue de l'allocation et de la gestion du boni pour enfant, l'article 7 du projet de loi a pour objet d'autoriser la création d'une base de données commune entre l'Administration des Contribution Directes (ACD) et la Caisse Nationale des Prestations Familiales (CNPF) dont la finalité consiste à permettre la détermination du droit à la modération d'impôt des enfants n'ayant pas bénéficié du boni pour enfant.

La Commission nationale se félicite de ce que les auteurs du projet de loi ont clairement précisé la finalité du fichier commun.

La mise en corrélation de données personnelles provenant des fichiers de l'ACD et de la CNPF constitue une interconnexion au sens de la loi sur la protection des données.

Les textes légaux ou réglementaires autorisant une interconnexion de données devraient respecter la ratio des dispositions de l'article 16 de la loi du 2 août 2002[6]. Ce dernier prévoit entre autres que « l'interconnexion des données doit permettre d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements ». La motivation dans le commentaire des articles fait ressortir un intérêt légitime consistant notamment à permettre la détermination du droit à la modération d'impôt des enfants n'ayant pas bénéficié du boni pour enfant. Selon le commentaire des articles, la création d'une base de données commune est « incontournable dans l'intérêt d'une gestion appropriée des droits des contribuables, étant donné que boni et modération pour enfant cohabiteront nécessairement et seront donc complémentaires ».

Remarquons toutefois que les deux administrations, qui partageront entre elles un certain nombre de données, poursuivent, de par leurs missions, des finalités correspondant à des intérêts publics différents. En outre, la CNPF recevra communication de données de l'ACD qui sont protégées par le secret fiscal. Les options retenues au départ dans la conception du boni pour enfant (mesure fiscale mais débouchant sur une allocation sui generis par le biais de la CNPF) ont comme conséquence qu'un partage de données entre les deux administrations sous forme d'interconnexion est la seule solution possible en pratique.

Dans un souci de respect de la protection des données et de la vie privée, le législateur devrait éviter autant que possible d'autoriser la mise en place successive d'interconnexions de fichiers d'administrations dont les missions correspondent à des intérêts publics différents. Le Conseil d'Etat, dans son avis du 30

6 doc. parl. N° 4735/13, p. 30

janvier 2007 relatif au projet de loi n° 5554 portant modification de la loi du 2 août 2002, reste lui aussi « *convaincu que l'interconnexion de données constitue une opération délicate devant être entourée d'un maximum de garanties* ». La délimitation précise des catégories de personnes et des renseignements les concernant qui doivent figurer dans la base de données commune constituent une telle garantie. L'article 7 alinéa 2 du projet de loi indique comme personnes concernées les allocataires, les attributaires et les enfants bénéficiant du boni pour enfant ainsi que les contribuables et enfants qui continuent à bénéficier de la modération d'impôt pour enfant. Cette garantie ne pourra être effective que si le terme « *notamment* » est supprimé dudit article.

La gestion partagée du fichier comporte par ailleurs un risque inhérent de dilution des responsabilités des deux administrations en question.

Au vu de cette considération, la Commission nationale recommande d'insérer à l'article 7 un alinéa supplémentaire relatif aux mesures de sécurité appropriées dont l'interconnexion devrait être assortie en tenant compte de la nature des données traitées. Elle suggère le libellé suivant : « *L'accès à cette base de données commune est limité à un nombre restreint de personnes autorisées. Le système informatique doit être sécurisé conformément aux articles 22 et 23 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel*. »

Avis de la Commission nationale pour la protection des données concernant le projet de règlement grand-ducal portant exécution de l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection Générale de la Police.

Délibération n°267/2007 du 14 décembre 2007

Conformément à l'article 32 paragraphe 3 lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après « la Commission nationale ») a notamment 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 de la Justice en date du 3 décembre 2007 que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de règlement grand-ducal prémentionné.

Le projet de règlement grand-ducal porte exécution de l'article 34-1 que le projet de loi n° 5563 entend insérer dans la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police. Ledit article 34-1 énumère les dix fichiers des personnes morales de droit public auxquels auront accès directement les magistrats du ministère public et les officiers de police judiciaire. Les articles 1 à 10 du projet de règlement grand-ducal sous examen déterminent de façon détaillée et limitative les données à caractère personnel des dix fichiers publics en question qui pourront être consultées. Les auteurs dudit projet estiment notamment le cadre normatif d'un règlement grand-ducal mieux adapté que celui d'une loi pour prévoir les dispositions de ce genre.

La Commission nationale a pris connaissance de l'avis du Conseil d'Etat du 23 octobre 2007 référencé n°47.243 et relatif au projet sous examen. Elle rejoint l'analyse et les observations faites par la Haute Corporation en ce qui concerne le statut juridique des informations – données judiciaires ou données policières (article 8 ou article 17 de la loi modifiée du 2 août 2002) – obtenues par voie d'accès aux dix fichiers de certaines personnes morales de droit public. Pareillement, elle estime que l'accès aux données de ces fichiers devrait plutôt être rattaché au régime de l'article 17 de la loi modifiée du 2 août 2002 qu'à celui de l'article 8 de la même loi.

Pour ce qui est de la délimitation des données susceptibles d'être consultées, la Commission nationale se félicite de ce que les auteurs du projet de règlement grand-ducal l'ont suivi dans ses recommandations formulées dans son avis[7] du 4 mai 2005, à savoir de prévoir une nomenclature précise des données auxquelles auraient accès les magistrats du ministère public et les officiers de police judiciaire

Ce souci de limiter ab initio les données visées dans les textes législatifs prévoyant une communication de données par accès direct d'une administration aux données d'une autre ou une interconnexion de fichiers publics, ne se retrouve malheureusement pas toujours dans d'autres initiatives législatives. La Commission nationale est toutefois confiante que les autorités, soucieuses du respect de la protection des données personnelles et de la vie privée, auront certainement à cœur d'en tenir compte davantage à l'avenir.

En termes de confidentialité des données et de sécurité des traitements au sens des articles 21 à 23 de la loi modifiée du 2 août 2002, le maître du fichier, c'est-à-dire, le responsable du traitement est en quelque sorte le gardien et des données et de la compatibilité des finalités des traitements. Il doit ainsi veiller à ce que la communication des données personnelles à un tiers se fasse selon le même principe de finalité et que l'utilisation des données reste compatible avec le traitement initial. Il devrait donc conserver la maîtrise sur les données contenues dans ses fichiers au lieu de les voir passivement accédées de l'extérieur.

7 Doc. parl. N° 5563/02 (avis relatif à l'avant-projet de loi)

Un accès direct par des tiers extérieurs à des données comporte non seulement des risques d'abus, mais également un risque de sécurité réduite découlant de la dilution des responsabilités au niveau des personnes accédant aux données. Afin d'éviter, ou du moins, de minimiser ces risques, des garanties appropriées et suffisantes doivent être prévues.

En l'espèce, la Commission nationale estime que le projet de règlement grand-ducal sous examen répond aux préoccupations déjà exprimées dans son avis du 4 mai 2005 précité, alors et surtout que le texte du projet de loi n° 5563 prévoit des garanties appropriées au niveau des procédés automatisés, à savoir le traçage (loggings) des accès opérés et le contrôle de ces derniers par l'autorité de contrôle instituée par l'article 17 paragraphe (2) de la loi modifiée du 2 août 2002.

Délibération n° 57/2007 du 25 mai 2007 de la Commission nationale pour la protection des données relative à la demande d'autorisation de l'Institut Luxembourgeois de Régulation concernant la procédure entièrement automatisée de l'accès de plein droit prévu par 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.

Vu 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.

Vu le Règlement grand-ducal du 21 décembre 2004 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.

Vu la Délibération n° 16/2004 du 12 mai 2004 de la Commission nationale pour la protection des données relative à la demande d'autorisation de l'Institut Luxembourgeois de Régulation concernant la procédure entièrement automatisée de l'accès de plein droit prévu par 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.

La première ébauche du système automatisé tel que défini par 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 n'a pas été retenue, raison pour laquelle l'Institut Luxembourgeois de Régularisation s'est vu forcé d'avoir recours à un autre fournisseur et de recommencer l'implémentation technique du système automatisé. Par conséquent, la délibération susmentionnée ne coïncide plus dans tous ses éléments au système tel qu'il se trouve actuellement dans sa phase finale de réalisation. Ainsi la Commission nationale pour la protection des données (ci-après dénommée « la Commission nationale ») a réexaminé l'architecture technique et fonctionnelle du système élaboré par l'Institut en vue d'assurer l'accès des autorités visées au paragraphe 1er de l'article 41 aux données d'identification des abonnés et utilisateurs, des opérateurs et fournisseurs de services de communications électroniques y visés par voie d'un accès informatique distant.

Elle a réexaminé le système proposé aussi bien du point de vue de la sécurisation des données que de l'organisation et du déroulement des procédures prévu qui doivent garantir la confidentialité tant des données contenues dans le système que des informations relatives à leur accès, consultation et mise à jour et permettre un contrôle approprié de la part de la Commission nationale susceptible d'éviter des abus ou dysfonctionnements, sinon de les constater le cas échéant.

Il résulte des explications fournies, que la conception choisie est logique et transparente, les mesures de sécurité techniques et organisationnelle appropriées et la facilité d'utilisation suffisante de façon à éviter des malentendus et erreurs de manipulation. L'architecture et les solutions techniques retenues nous paraissent de nature à préserver la confidentialité et l'intégrité des données ainsi que la traçabilité suffisante des opérations pour assurer la protection des données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés ainsi que contre toute autre forme de traitement illicite :

1) Architecture

L'architecture retenue est basée sur des logiciels libres «Open Source », ce qui présente l'avantage d'être disponible sous forme de code source et d'être ainsi librement redistribuable et modifiable.

2) Procédure entièrement automatisée du système d'information

La procédure entièrement automatisée permettant l'accès à distance par voie de communication électronique est décrite ci-après :

Transfert des données des opérateurs et fournisseurs de services

Le transfert journalier des données des opérateurs et fournisseurs de services vers l'Institut se fait moyennant « https upload ». Afin de pouvoir initier un transfert de données vers l'Institut, les opérateurs et fournisseurs de services doivent disposer d'un certificat électronique valide et être enregistrés au 'centre d'information'. Une fois déposés, les fichiers provenant des opérateurs ne peuvent plus être récupérés par ces derniers.

Les fichiers ainsi déposés par les opérateurs et fournisseurs de services au centre d'information sont vérifiés et transférés vers le moteur de bases de données (système interne hébergeant les données).

Les opérateurs et fournisseurs de services n'ont pas d'accès aux données enregistrées dans le centre d'information.

Le centre d'information renvoie pour chaque transfert de données un courrier électronique à l'émetteur du fichier, l'informant de la réception et de la validation du transfert des données.

Consultation du Centre d'Information par les autorités visées

Une application WEB permet aux autorités visées d'envoyer des requêtes au centre d'information. La communication est effectuée moyennant le protocole « https ».

L'application WEB est uniquement accessible à l'intérieur du réseau de l'Etat.

L'authentification sur la page WEB se fait moyennant un « username », un code pin et un « passcode » généré par un « hardware token RSA ».

La requête est envoyée à l'Institut, où elle est traitée et subdivisée en une enveloppe et un contenu permettant de sauvegarder et de consulter, de façon séparée, les informations y relatives.

Les informations faisant partie de l'enveloppe sont :

- l'identifiant de la personne effectuant la recherche, le numéro du dossier, la date et l'heure de la recherche et les informations concernant le contenu représentant le résultat de la requête retourné par le système automatisé.

Avant l'envoi de la réponse au requérant initial, l'enveloppe, ainsi que le contenu, sont stockés dans le système de contrôle (ci-après Système Anti-Abus, SAA) de manière chiffrée et dotée d'une signature électronique.

Au cas où le nombre de résultats dépasse une certaine limite, les résultats sont affichés de manière paginée et seulement les pages consultées sont sauvegardées dans le SAA.

L'application WEB permet à l'utilisateur de choisir la priorité du traitement, traitement direct ou traitement différé avec récupération postérieure du résultat.

Le système conserve, de façon chiffrée et non accessible à des tiers, les réponses à une requête pendant 24 heures, durée après laquelle les données respectives sont effacées. L'Institut n'a pas accès en clair aux données chiffrées contenues dans les réponses aux requêtes.

Consultation du Centre d'Information par les Centres d'Appels d'Urgence

La consultation des données à partir d'un Centre d'Appels d'Urgence se fait uniquement sur base des numéros d'appel entrants à la centrale d'appels d'urgence et uniquement sur des postes de travail destinés à cette fin. Les numéros entrants au Centre d'Appels d'Urgence ne sont transmis au Centre d'Information qu'en cas de besoin.

La communication entre le centre d'information et les Centres d'Appels d'Urgence se fait par l'intermédiaire d'un serveur qui collecte et transmet les requêtes provenant des postes respectifs. Le Centre d'Information accepte toutes les requêtes provenant des serveurs des Centre d'Appels d'Urgence disposant d'un certificat électronique valide et enregistré auprès du Centre d'Information.

Toute communication entre l'Institut et les différents Centre d'Appels d'Urgence est chiffrée par un protocole sécurisé.

Le centre d'information retourne le résultat aux Centre d'Appels d'Urgences sous format XML.

La requête est envoyée à l'Institut où elle est traitée et subdivisée en une enveloppe et un contenu permettant de sauvegarder et de consulter, de façon séparée, les informations y relatives. Les informations faisant partie de l'enveloppe sont l'identifiant de la personne effectuant la recherche, le numéro du dossier, la date et l'heure de la recherche et les informations concernant le contenu représentant le résultat de la requête retourné par le système automatisé. Avant l'envoi de la réponse au requérant initial, l'enveloppe ainsi que le contenu sont stockés dans le système de contrôle (ci-après Système Anti-Abus) de manière chiffrée et dotée d'une signature électronique.

3) Système Anti-Abus (contrôle)

L'architecture inclut une protection du système contre tout abus possible en provenance d'un utilisateur. A cette fin, un registre des requêtes est prévu. La consultation de ce registre est strictement limitée aux autorités ayant le pouvoir de contrôle et d'enquête. L'Institut n'est pas autorisé à consulter le contenu de ce registre. Conformément au « règlement grand-ducal du 21 décembre 2004 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 », chaque requête est subdivisée en une enveloppe et un contenu.

4) Disponibilité de l'application

L'architecture retenue se compose de trois systèmes informatiques indépendants :

- un environnement de développement,
- un environnement d'essais,
- un environnement de production.

L'équipement du système comprend plusieurs serveurs installés dans deux racks placés dans des salles informatiques distinctes. Une solution de cluster (système de haute disponibilité) a été choisie, de façon à ce qu'une disponibilité puisse être garantie 24/24 heures et 7/7 jours.

La conception du projet entier a été réalisée de façon à garantir une infrastructure satisfaisant aux critères d'une solution NSPOF (No Single Point Of Failure).

Statistiques

Le centre d'information permet de visualiser des statistiques anonymisées afin d'identifier tout problème dans l'infrastructure, ainsi que chaque déclin de performance.

Système audit

Le centre d'information enregistre les actions administratives qui sont effectuées sur le système.

5) Sécurisation du système

- contrôle à l'entrée des installations
  - accès au bâtiment sécurisé
  - accès aux salles serveurs sécurisé et restreint
- contrôle des supports
  - chiffrage des disques et des données
  - chiffrages des données sauvegardées sur bande magnétique
  - procédures de sauvegarde et de gestion des bandes magnétiques
- contrôle de la mémoire
  - certificats nécessaires pour déposer un fichier XML
  - « Système Anti-Abus (SAA)» registre des requêtes
  - Système d'audit – registre des actions administratives
- contrôle de l'utilisation
  - accès avec des tokens RSA (clients AV)
  - accès avec un certificat (clients CAU)
  - accès PCSAA à travers un HSM

- contrôle de l'accès

  - modèle de rôles pour toute catégorie d'utilisateurs possibles

- contrôle de la transmission

  - tokens d'accès RSA associés à des personnes physiques
  - certificat serveur pour les centrales d'urgences et transmission du username dans la requête
  - chiffrage des communications

- contrôle de l'introduction

  - « Système Anti-Abus (SAA)» registre des requêtes
  - Système d'audit – registre des actions administratives

- contrôle du transport

  - chiffrage de toute communication effectuée entre les différents serveurs du système
  - chiffrage de toute communication avec les clients du système

- contrôle de la disponibilité

  - sauvegarde des données « SAA » sur bande magnétique
  - retransmission des données opérateurs en cas de problème (pas de mise sur bande de ces données)
  - clustering au niveau serveurs pour garantir la disponibilité du service et des données temporaires.

Les mesures décrites dans la documentation fournie et expliquée par l'Institut suffisent aux exigences de la sécurisation tant au niveau du matériel que des logiciels, notamment du système d'exploitation, des données ainsi que des communications réseaux.

***

Compte tenu des développements qui précèdent, la Commission nationale, réunissant ses trois membres effectifs et délibérant à l'unanimité des voix :

partant autorise l'Institut Luxembourgeois de Régulation à mettre en place le système décrit dans sa demande ayant pour objet de permettre l'accès automatisé des autorités visées à l'article 41 de la loi aux données d'identification des abonnés et utilisateurs des services de communication électronique, ces données étant fournies par les opérateurs et fournisseurs de services et étant actualisées au moins une fois par jour conformément à l'article 41 de la loi et aux règlements d'application pris sur sa base ;

Délibération n°63/2007 du 22 juin 2007
Autorisation unique relative aux traitements de données à caractère personnel portant sur le contrôle des horaires de travail dans le cadre d'une organisation de travail selon l'horaire mobile

La Commission nationale pour la protection des données (ci-après dénommée « Commission nationale ») :

Vu 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 ;

Vu 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 ») ;

Vu le Code du travail, et notamment ses articles : L.261-1, L.261-2 et L.423-1 ;

Considérant que les systèmes de contrôle des horaires de travail sont destinés à la gestion et le contrôle des horaires de travail et des temps de présence sur le lieu de travail ;

que ces systèmes mis en œuvre peuvent utiliser la technique des cartes magnétiques ou à puce, avec ou sans contact, ou d'autres techniques de pointage tels que la saisie d'un code secret sur un terminal ou une console ;

qu'ils permettent ainsi de contrôler et de vérifier la date et l'heure d'utilisation de la carte ou du code afin d'effectuer un décompte des heures de travail prestées par chaque personne concernée et de connaître exactement la présence et les absences des travailleurs sur le lieu de travail ;

que ces cartes ou codes permettent d'identifier directement ou indirectement l'agent détenteur de la carte ou du code ;

que la surveillance est définie à l'article 2 lettre (q) de la loi 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*» ;

qu'il s'ensuit que le contrôle des horaires de travail par badge/carte ou code, permettant d'identifier l'agent détenteur, constitue un traitement de données à caractère personnel à des fins de surveillance au sens des articles 10 de la loi et L.261-1 du Code du travail ;

que suivant les dispositions de l'article 14 paragraphe (1) lettre (a), les traitements prévus aux articles 10 de la loi du 2 août 2002 et L.261-1 du Code du Travail, concernant les traitements à des fins de surveillance, sont soumis au régime de l'autorisation préalable de la Commission nationale ;

que, dès lors, seuls sont soumis à autorisation préalable les traitements faisant appel à des moyens techniques ou informatiques, et que, par conséquent, les traitements manuels relatifs à un tel contrôle relèvent du régime de la notification préalable (articles 12 et 13 de la loi du 2 août 2002) ;

Considérant qu'en vertu de l'article 14 paragraphe (3) de la loi du 2 août 2002, la Commission nationale peut autoriser par une décision unique les traitements qui ont une même finalité, qui portent sur des données identiques et ont les mêmes destinataires ou catégories de destinataires ;

que la Commission nationale, consciente du fait qu'un nombre important d'employeurs ont mis en place une organisation de travail selon l'horaire mobile et soucieuse de faciliter les formalités administratives préalables à remplir par les responsables du traitement, souhaite simplifier et accélérer la mise en conformité des responsables du traitement avec les dispositions de la loi du 2 août 2002 en ce qui concerne ces systèmes de surveillance ;

Considérant que la présente décision unique a pour objet l'autorisation de l'ensemble des traitements de données en question qui correspondent aux conditions et circonstances décrites ci-après ;

Considérant que tout traitement, qui par un élément quelconque n'est pas strictement conforme aux

présentes dispositions doit faire l'objet d'une demande d'autorisation préalable au sens de l'article 14 paragraphes (1) et (2) de la loi du 2 août 2002 ;

Considérant que sont exclus de la présente autorisation unique les systèmes utilisant une identification biométrique ;

Décide que les responsables du traitement qui adressent à la Commission nationale un engagement formel de conformité pour leurs traitements de données à caractère personnel à des fins de surveillance et à des fins de surveillance sur le lieu de travail répondant aux conditions fixées par la présente autorisation unique sont autorisés à mettre en œuvre ces traitements.

Généralités

La présente autorisation unique ne concerne que les systèmes de surveillance des horaires de travail dans le cadre d'une organisation de travail selon l'horaire mobile, c'est-à-dire ceux qui permettent la gestion et le contrôle des horaires de travail et des temps de présence sur le lieu de travail.

Le traitement mis en œuvre par la personne physique ou la personne morale, de droit public ou privé, qui est responsable du traitement (ci-après « le responsable du traitement ») ne doit concerner que les arrivées sur le lieu de travail et les départs du lieu de travail.

La référence au terme « *travailleurs* » dans la présente autorisation unique inclut aussi bien les salariés, y compris les apprentis, les travailleurs intérimaires et les stagiaires, que les fonctionnaires ou autres agents publics et généralement toute personne travaillant sous un lien de subordination juridique à l'égard du responsable du traitement.

La référence au terme « *tiers* » dans la présente autorisation unique inclut aussi bien les fournisseurs, les visiteurs, les clients, que les prestataires de services et généralement toute personne qui ne se trouve pas soumis à un lien de subordination juridique par rapport au responsable du traitement.

Finalités du traitement

Le traitement ne doit pas avoir d'autres finalités que :

la gestion des horaires de travail ;

le contrôle des temps de présence sur le lieu de travail.

Condition de légitimité du traitement

Dérogeant à l'article 5 relatif aux conditions de légitimité générales, les articles 10 de la loi du 2 août 2002 et L.261-1 paragraphe (1) du Code du Travail, énumèrent les cas d'ouverture limitatifs permettant une surveillance en général et une surveillance spécifique sur le lieu de travail.

Le traitement de données à caractère personnel à des fins de surveillance sur le lieu de travail peut être mis en œuvre par l'employeur s'il en est le responsable. Un tel traitement n'est possible que s'il est nécessaire dans le cadre d'une organisation de travail selon l'horaire mobile conformément à la loi.

Sont donc visés tous les traitements de données effectués à l'aide des dispositifs décrits ci-dessus en vue du contrôle des horaires de présence des travailleurs, de leur identification à leur entrée et sortie, des plages obligatoires, de la vérification du respect des règles de compensation et de leur incidence sur la rémunération et la compensation des congés.

Par ailleurs, le traitement de données à caractère personnel portant sur les travailleurs du responsable du traitement sera considéré comme légitime dans le cadre de l'article L.261-1 du Code du Travail, sous réserve d'avoir obtenu préalablement l'accord du comité mixte, le cas échéant institué, conformément aux dispositions de l'article L.423-1 dudit Code.

Le traitement de données à caractère personnel portant sur les tiers ne pourra être effectué que si la personne concernée a donné son consentement.

Il convient de relever que la surveillance des horaires de travail et des temps de présence sur le lieu de travail ne concerne en principe que les travailleurs du responsable du traitement. Il existe cependant des situations exceptionnelles où des tiers (p.ex. les employés d'un sous-traitant) effectuent des prestations au sein des locaux du responsable du traitement et sont, à ce titre, soumis à une telle surveillance, notamment pour vérifier la conformité aux contrats de services souscrits par le responsable du traitement.

Au regard du catalogue limitatif de conditions de légitimité énumérées à l'article 10, la Commission nationale retient que la seule condition de légitimité susceptible de trouver application pour légitimer la surveillance des heures de présence de tiers travaillant dans les locaux du responsable du traitement est la lettre (a) de l'article 10 paragraphe 1er de la loi.

La définition du consentement figurant à l'article 2 lettre (c) de la loi étant plus rigoureuse que celle de la directive 95/46/CE (consentement exprès et non équivoque) ne permet pas de déduire un consentement implicite du comportement des intervenants externes qui enregistrent leurs entrées et sorties conformément au système décrit dans la demande.

Il découle de ce qui précède qu'une surveillance relative aux tiers intervenant au sein du responsable du traitement ne pourra être considérée comme légitime que sous la condition exclusive que le responsable du traitement dispose de leur consentement au sens de la définition de l'article 2 lettre (c) de la loi du 2 août 2002.

Données collectées et traitées

Chaque application peut être mise en œuvre de façon indépendante ou intégrée. A l'exclusion des données biométriques, les données suivantes peuvent être traitées :

- identité : nom, prénom, photographie, numéro d'identification ou de matricule interne ;
- vie professionnelle : service de rattachement, fonction ;
- badges : numéro du badge ou de la carte, date de validité ;
- temps de présence : heures d'entrée et de sortie, plages horaires habituellement autorisées, numéro de la porte, du terminal ou de la borne utilisée, cumul des horaires, heures supplémentaires, autorisation d'absences, congés, autres absences (motifs et décomptes).

Les données recueillies doivent être traitées loyalement et ne doivent être utilisées que pour les finalités sur lesquelles est fondée la présente décision unique.

Durée de conservation

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.

Une durée limitée de conservation de données constitue une garantie supplémentaire pour éviter d'éventuels détournements de finalité.

Les données personnelles des travailleurs salariés et assimilés ne doivent pas être conservées au-delà de trois ans.

Ce délai est conforme aux dispositions de l'article 2277 du Code Civil, selon lesquelles les actions en paiement des rémunérations de toute nature dues au salarié se prescrivent par trois ans. Pendant ce délai l'employeur pourra conserver les données relatives au contrôle des horaires de travail pouvant servir comme éléments de preuve en cas de contestations, revendications ou réclamations émanant des salariés.

Les données personnelles des agents publics ne doivent pas être conservées au-delà de cinq ans.

Ce délai met en œuvre les apports de la jurisprudence luxembourgeoise en matière administrative, qui retient que le nouvel alinéa premier de l'article 2277 du code civil n'a pas apporté de changement à l'applicabilité du dernier alinéa du même article, selon lequel les traitements et indemnités des fonctionnaires et agents des organismes de droit public se prescrivent par cinq ans (cf. Cour administrative, arrêt du 11 juin 1998, rôle 10607C).

Dans l'hypothèse d'une contestation ou d'un incident, les données s'y rapportant ne font pas l'objet de l'obligation de destruction au bout des délais susmentionnés, dans le cadre de la transmission des données aux autorités compétentes, visées à l'article 10 paragraphe (3).

Destinataires des informations

Dans la limite de leurs attributions respectives, les informations nominatives peuvent être communiquées aux destinataires suivants :

- les membres de la direction ;
- les personnes habilitées du service du personnel ;
- les personnes habilitées du service en charge du calcul des salaires ou des traitements ;
- les personnes habilitées des services en charge de la sécurité des locaux.

Aucune communication des données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire ou encore aux fins de la gestion normale d'entreprise.

Pays tiers à destination desquels les transferts de données sont envisagés

Aucune donnée à caractère personnel visée dans la présente autorisation unique ne doit être transférée à destination de pays tiers (hors Union européenne) n'assurant pas un niveau de protection adéquat.

Le transfert peut néanmoins être effectué vers les Etats qui n'assurent pas un niveau de protection adéquat suffisant et notamment reconnu comme tel par une décision de la Commission européenne sous réserve du respect par le responsable du traitement des dispositions prévues aux articles 18 et 19 de la loi du 2 août 2002. Tout contrat conclu avec les personnes habilitées à obtenir communication des données devra respecter les décisions de la Commission européenne relatives aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers ou des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du 24 octobre 1995.

Information et droit d'accès

L'information des personnes concernées sur les finalités et les fonctions du traitement, les destinataires des informations et les modalités d'exercice de leur droit d'accès et de rectification doit être assurée par tout moyen approprié, notamment par la diffusion d'une note explicative.

Conformément aux dispositions de l'article L.261-1 paragraphe (1) deuxième alinéa et sans préjudice du droit à l'information de la personne concernée visé à l'article 26 de la loi du 2 août 2002, « sont informés préalablement par l'employeur : la personne concernée, ainsi que pour les personnes tombant sous l'empire de la législation sur le contrat de droit privé : le comité mixte ou, à défaut, la délégation du personnel ou, à défaut encore, l'Inspection du travail et des mines ; pour les personnes tombant sous l'empire d'un régime statutaire : les organismes de représentation du personnel tels que prévus par les lois et règlements afférents.

Mesures de sécurité et sous-traitance

Des mesures de sécurité organisationnelles et techniques suffisantes doivent être prises, conformément aux articles 22 et 23 de la loi du 2 août 2002, afin d'assurer la protection des données traitées 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 forme de traitement illicite.

L'ensemble des mesures prises pour assurer la sécurité du traitement en application des articles 22 et 23 de la loi du 2 août 2002 doit conférer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger, le tout en fonction du risque d'atteinte à la vie privée, ainsi que de l'état de l'art et des coûts liés à la mise en œuvre dudit traitement.

Lorsque le responsable du traitement s'adjoint les services d'un sous-traitant pour la mise en œuvre du traitement, un contrat ou un acte juridique écrit conforme aux dispositions de l'article 22, paragraphe (3) doit être signé.

Délibération n°64/2007 du 22 juin 2007
Autorisation unique relative aux traitements de données à caractère personnel portant sur la surveillance des accès

La Commission nationale pour la protection des données (ci-après dénommée « Commission nationale ») :

Vu 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 ;

Vu 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 ») ;

Vu le Code du travail, et notamment ses articles : L.261-1, L.261-2 et L.423-1 ;

Considérant que les systèmes de surveillance des accès sont destinés à la gestion et au contrôle des accès physiques à l'entrée de sites et bâtiments et dans certaines zones limitativement identifiées qui font l'objet d'une restriction de circulation à l'intérieur de ces sites et bâtiments ;

que ces systèmes mis en œuvre peuvent utiliser la technique des cartes magnétiques ou à puce, avec ou sans contact, ou d'autres techniques de pointage tels que la saisie d'un code secret sur un terminal ou une console ;

que ces cartes ou codes permettent d'identifier directement ou indirectement l'agent détenteur de la carte ou du code ;

que la surveillance est définie à l'article 2 lettre (q) de la loi 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*» ;

qu'il s'ensuit que le contrôle des accès par badge/carte ou code, permettant d'identifier l'agent détenteur, constitue un traitement de données à caractère personnel à des fins de surveillance au sens des articles 10 de la loi et L.261-1 du Code du travail ;

que suivant les dispositions de l'article 14 paragraphe (1) lettre (a), les traitements prévus aux articles 10 de la loi du 2 août 2002 et L.261-1 du Code du Travail, concernant les traitements à des fins de surveillance, sont soumis au régime de l'autorisation préalable de la Commission nationale ;

que, dès lors, seuls sont soumis à autorisation préalable les traitements faisant appel à des moyens techniques ou informatiques, et que, par conséquent, les traitements manuels relatifs à un tel contrôle relèvent du régime de la notification préalable (articles 12 et 13 de la loi du 2 août 2002) ;

Considérant qu'en vertu de l'article 14 paragraphe (3) de la loi du 2 août 2002, la Commission nationale peut autoriser par une décision unique les traitements qui ont une même finalité, qui portent sur des données identiques et ont les mêmes destinataires ou catégories de destinataires ;

que la Commission nationale, consciente du fait qu'un nombre important d'employeurs ont mis en place des systèmes automatisés de contrôle d'accès et soucieuse de faciliter les formalités administratives préalables à remplir par les responsables du traitement, souhaite simplifier et accélérer la mise en conformité des responsables du traitement avec les dispositions de la loi du 2 août 2002 en ce qui concerne ces systèmes de surveillance ;

Considérant que la présente décision unique a pour objet l'autorisation de l'ensemble des traitements de données en question qui correspondent aux conditions et circonstances décrites ci-après ;

Considérant que tout traitement qui par un élément quelconque n'est pas strictement conforme aux présentes dispositions doit faire l'objet d'une demande d'autorisation préalable au sens de l'article 14 paragraphes (1) et (2) de la loi du 2 août 2002 ;

Considérant que sont exclus de la présente autorisation unique les systèmes utilisant une identification biométrique ;

Décide que les responsables du traitement qui adressent à la Commission nationale un engagement formel de conformité pour leurs traitements de données à caractère personnel à des fins de surveillance et à des fins de surveillance sur le lieu de travail répondant aux conditions fixées par la présente autorisation unique sont autorisés à mettre en œuvre ces traitements.

Généralités

La présente autorisation unique ne concerne que les systèmes de surveillance des accès, c'est-à-dire ceux qui permettent la gestion, l'organisation et l'administration des contrôles des accès physiques à l'entrée de sites et bâtiments ainsi que dans certaines zones limitativement identifiées qui font l'objet d'une restriction de circulation à l'intérieur de ces sites et bâtiments.

Le traitement mis en œuvre ne doit concerner que les entrées et sorties des sites et bâtiments des responsables du traitement de droit public ou privé (ci-après « le responsable du traitement ») et ne pas permettre le contrôle des déplacements à l'intérieur du lieu de travail, à l'exception des cas dans lesquels certaines zones identifiées font l'objet d'une restriction de circulation justifiée par la sécurité des biens et des personnes qui y travaillent.

La référence au terme « *travailleurs* » dans la présente autorisation unique inclut aussi bien les salariés, y compris les apprentis, les travailleurs intérimaires et les stagiaires, que les fonctionnaires ou autres agents publics et généralement toute personne travaillant sous un lien de subordination juridique à l'égard du responsable du traitement.

La référence au terme « *tiers* » dans la présente autorisation unique inclut aussi bien les fournisseurs, les visiteurs, les clients, que les prestataires de services et généralement toute personne qui ne se trouve pas soumis à un lien de subordination juridique par rapport au responsable du traitement.

Finalités du traitement

Le traitement ne doit pas avoir d'autre finalité que de permettre l'accès aux seules personnes autorisées, en l'occurrence :

le contrôle des accès des travailleurs et des tiers aux sites et bâtiments du responsable du traitement ;

le contrôle des accès des travailleurs et des tiers aux locaux ou zones limitativement identifiés du responsable du traitement faisant l'objet d'une restriction de circulation.

Conditions de légitimité du traitement

Dérogeant à l'article 5 relatif aux conditions de légitimité générales, les articles 10 de la loi du 2 août 2002 et L.261-1 paragraphe (1) du Code du Travail, énumèrent les cas d'ouverture limitatifs permettant une surveillance en général et une surveillance spécifique sur le lieu de travail.

Le traitement de données à caractère personnel à des fins de surveillance sur le lieu de travail peut être mis en œuvre par l'employeur s'il en est le responsable. Un tel traitement, portant sur les travailleurs, n'est possible que s'il est nécessaire :

- pour les besoins de sécurité et de santé des travailleurs, sous réserve d'avoir obtenu préalablement l'accord du comité mixte, le cas échéant institué, ou
- pour les besoins de protection des biens de l'entreprise.

Le traitement de données à caractère personnel portant sur les tiers ne pourra être effectué que :

- si la personne concernée a donné son consentement (au sens de la définition de l'article 2 lettre (c) de la loi du 2 août 2002), ou
- aux abords ou dans tout lieu accessible ou non au public autres que les locaux d'habitation, notamment dans les parkings couverts, les gares, aérogares et les moyens de transports publics, pourvu que le lieu en question présente de par sa nature, sa situation, sa configuration ou sa fréquentation un risque rendant le traitement nécessaire à la sécurité des usagers ainsi qu'à la prévention des accidents, ou
- aux lieux d'accès privé dont la personne physique ou morale y domiciliée ou établie est le responsable du traitement.

Données collectées et traitées

Chaque application peut être mise en œuvre de façon indépendante ou intégrée. A l'exclusion des données biométriques, les données suivantes peuvent être traitées :

- identité : nom, prénom, photographie, numéro d'identification ou de matricule interne ;
- vie professionnelle : zones d'accès habituellement autorisées, service de rattachement, fonction, société d'appartenance ;
- badges : numéro du badge ou de la carte, date de validité ;
- en cas d'accès à un parking : numéro d'immatriculation du véhicule, numéro de place de stationnement ;
- déplacement des personnes : heures d'entrée et de sortie, numéro de la porte, du terminal ou de la borne utilisée.

Les données recueillies doivent être traitées loyalement et ne doivent être utilisées que pour les finalités sur lesquelles est fondée la présente décision unique.

Durée de conservation

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.

Une durée limitée de conservation de données constitue une garantie supplémentaire pour éviter d'éventuels détournements de finalité.

Les données ne doivent pas être conservées plus de trois mois à compter de leur enregistrement, à moins que le traitement porte en même temps sur le contrôle des horaires de travail dans le cadre d'une organisation de travail selon l'horaire mobile. Dans ce cas, le responsable du traitement doit également signer l'engagement formel de conformité annexé à la délibération n°63/2007 du 22 juin 2007 intitulé « Autorisation unique relative aux traitements de données à caractère personnel portant sur le contrôle des horaires de travail » et respecter l'intégralité des conditions décrites dans ladite autorisation.

Dans l'hypothèse d'une contestation ou d'un incident, les données s'y rapportant ne font pas l'objet de l'obligation de destruction au bout des délais susmentionnés, dans le cadre de la transmission des données aux autorités compétentes, visées à l'article 10 paragraphe (3).

Destinataires des informations

Dans la limite de leurs attributions respectives, les informations nominatives peuvent être communiquées aux destinataires suivants :

- les membres de la direction ;
- les personnes habilitées du service du personnel ;
- les personnes habilitées des services en charge de la sécurité des locaux.

Aucune communication des données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire ou encore aux fins de la gestion normale d'entreprise.

Pays tiers à destination desquels les transferts de données sont envisagés

Aucune donnée à caractère personnel visée dans la présente autorisation unique ne doit être transférée à destination de pays tiers (hors Union européenne) n'assurant pas un niveau de protection adéquat.

Le transfert peut néanmoins être effectué vers les Etats qui n'assurent pas un niveau de protection adéquat suffisant et notamment reconnu comme tel par une décision de la Commission européenne sous réserve du respect par le responsable du traitement des dispositions prévues aux articles 18 et 19 de la loi du 2 août 2002. Tout contrat conclu avec les personnes habilitées à obtenir communication des données devra respecter les décisions de la Commission européenne relatives aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers ou des sous-traitants établis dans des pays

tiers en vertu de la directive 95/46/CE du 24 octobre 1995.

Information et droit d'accès

L'information des personnes concernées sur les finalités et les fonctions du traitement, les destinataires des informations et les modalités d'exercice de leur droit d'accès et de rectification doit être assurée par tout moyen approprié, notamment par la diffusion d'une note explicative.

Conformément aux dispositions de l'article L.261-1 paragraphe (1) deuxième alinéa et sans préjudice du droit à l'information de la personne concernée visé à l'article 26 de la loi du 2 août 2002, « sont informés préalablement par l'employeur : la personne concernée, ainsi que pour les personnes tombant sous l'empire de la législation sur le contrat de droit privé : le comité mixte ou, à défaut, la délégation du personnel ou, à défaut encore, l'Inspection du travail et des mines ; pour les personnes tombant sous l'empire d'un régime statutaire : les organismes de représentation du personnel tels que prévus par les lois et règlements afférents.

Mesures de sécurité et sous-traitance

Des mesures de sécurité organisationnelles et techniques suffisantes doivent être prises, conformément aux articles 22 et 23 de la loi du 2 août 2002, afin d'assurer la protection des données traitées 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 forme de traitement illicite.

L'ensemble des mesures prises pour assurer la sécurité du traitement en application des articles 22 et 23 de la loi du 2 août 2002 doit conférer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger, le tout en fonction du risque d'atteinte à la vie privée, ainsi que de l'état de l'art et des coûts liés à la mise en œuvre dudit traitement.

Lorsque le responsable du traitement s'adjoint les services d'un sous-traitant pour la mise en œuvre du traitement, un contrat ou un acte juridique écrit conforme aux dispositions de l'article 22, paragraphe (3) doit être signé.

Délibération n°108/2007 « élections sociales » du 14 septembre 2007 portant notification unique pour les traitements de données à caractère personnel (y compris certaines catégories particulières de données visés à l'article 6 paragraphe 1) opérés par les employeurs dans le cadre de l'organisation et du déroulement des élections des délégués du personnel, des délégations des jeunes travailleurs et des représentants du personnel dans les comités mixtes d'entreprise et les conseils d'administration des sociétés anonymes.

La Commission nationale pour la protection des données (ci-après dénommée « Commission nationale ») ;

Vu la loi du 27 juillet 2007 portant modification de la loi du 2 août 2002 relative à la protection des personnes à l'égard des traitements de données à caractère personnel,

Vu les articles 4, 5, 6, 12 et 13 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci après « la loi du 2 août 2002 ») et notamment le paragraphe (4) de l'article 13 ;

Vu les articles L.411-1 et suivants du Code du Travail et le règlement grand-ducal modifié du 21 septembre 1979 concernant les opérations électorales pour la désignation des délégués du personnel ;

Vu les articles L.421-1 et suivants du Code du Travail et le règlement grand-ducal du 24 septembre 1974 concernant les opérations électorales pour la désignation des représentants du personnel dans les comités mixtes d'entreprises et les conseils d'administration des sociétés anonymes ;

Considérant que l'organisation et le déroulement des élections des délégués du personnel, des délégations des jeunes travailleurs et des représentants du personnel dans les comités mixtes d'entreprise et les conseils d'administration des sociétés anonymes ainsi que la proclamation des résultats de ces élections amènent les employeurs à enregistrer et traiter les données à caractère personnel relatives aux salariés et apprentis de l'entreprise et aux candidats qui se présentent pour les différents mandats à pourvoir ainsi qu' aux mandataires et présentateurs de chaque liste de candidats,

que tel est le cas notamment dans l'accomplissement des devoirs revenant aux chefs d'entreprise, conformément à la législation en vigueur au niveau de la constatation des effectifs à représenter, de la détermination du nombre de délégués à élire et des conditions de l'électorat actif et passif, de l'établissement des listes électorales, de la réception et publication des candidatures, de l'établissement des bulletins de vote, des opérations électorales proprement dites, du dépouillement du scrutin, de l'établissement et de la publication des résultats, de l'attribution des sièges ainsi que dans le cadre du contentieux éventuel auquel donneront lieu les élections sociales ;

que certaines des données traitées sont de la nature de celles visées à l'article 6 paragraphe 1er de la loi du 2 août 2002 comme catégories particulières de données (données sensibles) ;

Considérant que les traitements auxquels les données sont soumises par les différents employeurs du secteur privé, sont tous du même type de sorte qu'il paraît justifié d'en simplifier la façon de les notifier à la Commission nationale,

que ces traitements ont tous la même finalité, sont exercés dans le même cadre légal et portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires,

qu'il appert que la Commission nationale peut décider qu'ils feront l'objet d'une notification unique conformément à l'article 13 paragraphe (4) qui précise les conditions à respecter et mesures, notamment de sécurité, à appliquer dans la mise en œuvre du traitement, conformément à l'article 13 paragraphe (4) de la loi du 2 août 2002,

qu'il appartiendra par la suite aux employeurs désireux de se conformer à la loi du 2 août 2002 et de notifier

ledit traitement de données en bonne et due forme à la Commission nationale sous la forme d'un simple engagement formel de conformité [prévu à l'article 13 paragraphe (4) de la loi du 2 août 2002] à la description figurant dans la présente décision qui en énumère par ailleurs les conditions à respecter dans la mise en œuvre du traitement.

***

Décide :

Article 1 Généralités

Conformément à l'article 6 de la loi du 2 août 2002, tout traitement de données à caractère personnel susceptible de révéler notamment l'appartenance syndicale est interdit, sauf s'il est légitimé sur base des conditions visées à l'article 6 paragraphe (2) lettres (a) à (f) de la loi du 2 août 2002 qui sont invoqués. Il doit dans ce cas faire l'objet d'une notification comprenant les indications prévues à l'article 13 de la loi et faisant référence aux circonstances et conditions visées à l'article 6 paragraphe (2) de la loi du 2 août 2002.

L'organisation et le déroulement des élections des délégations du personnel, des délégations des jeunes travailleurs et des représentants du personnel dans les comités mixtes et les conseils d'administration, la publication des résultats et le contentieux éventuel y afférent conduisent nécessairement les chefs d'établissement et leurs délégués à inclure dans les traitements qu'ils opèrent en application de la législation sociale des données relatives à l'appartenance syndicale des personnes qui sont présentées sur les listes de candidats ou mandataires et présentateurs de ces listes.

Par ailleurs, la computation des effectifs pour la détermination des mandats à pourvoir et l'établissement des listes électorales renseignant sur les conditions de l'électorat actif et passif constituent des obligations pesant sur les employeurs et chefs d'établissement parmi les devoirs relatifs à l'organisation des élections sociales, au déroulement des opérations électorales mis à leur charge par la législation en vigueur. Ces opérations impliquent nécessairement un traitement de données à caractère personnel qui doit faire l'objet d'une notification préalable par le responsable du traitement en application des articles 12 et 13 de la loi du 2 août 2002.

Comme ce traitement est étroitement lié avec celui décrit précédemment et comme les finalités afférentes portent à chaque fois sur l'organisation des élections sociales, la préparation et le déroulement des opérations électorales et les devoirs à remplir dans ce contexte par les employeurs et chefs d'établissement en application de leur obligation légale, il apparaît indiqué d'inclure ces traitements dans une même décision unique.

La Commission nationale entend par la présente décision prévoir la déclaration par notification unique de tous traitements qui seront opérés par les employeurs et chefs d'établissements dans le cadre des élections sociales et pour lesquels ces derniers lui adresseront l'engagement formel de conformité prévu à l'article 13 paragraphe (4) en vue de notifier leurs traitements prévus dans la présente décision unique.

Article 2 Conditions et Modalités des traitements

a) Les responsables des traitements

Sont à considérer comme responsables des traitements les employeurs – personnes physiques ou morales – qui opèrent lesdits traitements en application des obligations relatives à l'organisation et au déroulement des élections des délégués du personnel, des délégations des jeunes travailleurs et représentants du personnel dans les comités mixtes d'entreprise et les conseils d'administration mises à charge des employeurs et chefs d'établissement en application de la législation en vigueur.

b) Condition de légitimité du traitement

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 6 paragraphe (2) de la loi du 2 août 2002, sous les lettres

b) et e) sont réunies dans le chef des responsables des traitements :

(b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail dans la mesure où il est autorisé par la loi, et/ou

(e) le traitement porte sur des données manifestement rendues publiques par la personne concernée.

c) Finalité(s) du traitement

L'organisation conformément à la loi des élections relatives à l'organisation et au déroulement des élections des délégués du personnel, des délégations des jeunes travailleurs et des représentants du personnel dans les comités mixtes d'entreprise et les conseils d'administration ainsi que l'accomplissement des tâches et devoirs relevant dans ce contexte de la responsabilité de l'employeur respectivement du chef d'établissement ou de son délégué.

d) Description détaillée des données ou catégories de données et des traitements auxquels elles sont soumises

Les données relatives aux électeurs, aux présentateurs et mandataires des listes de candidats et à ces derniers, notamment dans le cadre des documents suivants :

listes alphabétiques indiquant le nom, prénom, date de naissance et ancienneté des électeurs admis à l'électorat actif ou / et passif dans l'entreprise/ établissement ;

affiche reproduisant les candidatures conformément aux dispositions de :

l'article 10 du règlement grand-ducal modifié du 21 septembre 1979 concernant les opérations électorales pour la désignation des délégués du personnel,

l'article 10 du règlement grand-ducal modifié du 24 septembre 1974 concernant les opérations électorales pour la désignation des représentants du personnel dans le comité mixte d'entreprise et les conseils d'administration ;

bulletins de vote ;

listes de dépouillement et procès-verbaux ;

communications et/ou publications faisant connaître les résultats du scrutin.

Les traitements doivent :

ne porter que sur des données objectives aisément contrôlables par les intéressés grâce à l'exercice du droit individuel d'accès ;

n'appliquer à ces données que des logiciels dont les résultats peuvent être facilement contrôlés ;

ne pas donner lieu à des interconnexions autres que celles expressément prévues par un texte légal ;

ne pas donner lieu à des rapprochements autres que ceux nécessaires à l'accomplissement des devoirs compris dans la finalité énoncée au point c) ci-dessus ;

satisfaire en outre aux conditions énoncées aux points e) à j) ci-dessous.

Les données collectées et traitées doivent être adéquates, pertinentes et non excessives au regard de l'objet de l'organisation des élections des délégués du personnel, des délégations des jeunes travailleurs et des représentants du personnel dans les comités mixtes d'entreprise et les conseils d'administration aussi que l'accomplissement des tâches et devoirs relevant dans ce contexte de la responsabilité de l'employeur respectivement du chef d'établissement ou de son délégué.

e) Origine des données

Les données individuelles concernant exclusivement les travailleurs sous contrat de louage de services ou d'apprentissage ont été fournies par les concernés dans le cadre de la conclusion et de l'exécution de leur contrat d'emploi ou d'apprentissage.

Les données à caractère personnel relatives aux présentateurs, mandataires et candidats auront été fournies par ceux-ci (i.e. manifestement rendues publiques) dans le cadre de la présentation de candidatures sous les formes prévues par la loi (art.5 du règlement grand-ducal modifié du 21 septembre 1979 concernant les opérations électorales pour la désignation des délégués du personnel / art. 6 du règlement grand-ducal modifié du 24 septembre 1974 concernant les

opérations électorales pour la désignation des représentants du personnel dans les comités mixtes d'entreprise et les conseils d'administration).

f) Description des catégories de personnes concernées

Personnel sous contrat de travail (sauf celui sous contrat d'apprentissage), les salariés travaillant à temps partiel, les salariés sous contrat à durée déterminée et les travailleurs mis à disposition dans la mesure où les concernés entrent en ligne de compte pour le calcul des effectifs du personnel occupé dans l'entreprise ou de l'établissement.

Personnel sous contrat de louage de services ou d'apprentissage dans la mesure où les concernés sont électeurs/éligibles.

Présentateurs, mandataires et candidats figurant sur les listes présentées pour lesdites élections.

g) Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication de données à des tiers autres que ceux énumérés ci-après ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire, ou encore aux fins de la gestion normale d'entreprise :

- les concernés eux-mêmes
- le personnel
- l'Inspection du Travail et des Mines
- les syndicats présentant des candidats
- la/les délégations élues
- le comité mixte
- le conseil d'administration

h) Pays tiers à destination desquels des transferts de données sont envisagés

Les données à caractère personnel faisant l'objet de traitements dans le cadre de l'organisation et du déroulement des élections sociales ne doivent pas être transférées à destination de pays tiers (hors Union européenne)

i) Description détaillée permettant d'apprécier le respect des mesures de sécurité prévues aux articles 22 et 23

Pour l'essentiel la procédure électorale fait l'objet d'un traitement manuel sauf que les données issues du signalétique des ouvriers/employés et apprentis de l'entreprise font l'objet d'un traitement informatique en vue de la détermination du corps électoral et de la confection des listes d'électeurs et d'éligibles. Les dossiers, documents, listes et données appréhendés sous forme automatisées doivent faire l'objet de mesures de sécurité organisationnelles et techniques suffisantes conformément aux articles 19 à 24 de la loi du 2 août 2002.

L'ensemble des mesures prises pour assurer la sécurité du traitement en application des articles 22 et 23 de la loi du 2 août 2002 doit conférer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger, le tout en fonction du risque d'atteinte à la vie privée, ainsi que de l'état de l'art et des coûts liés à la mise en œuvre dudit traitement.

j) 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 pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

Conformément à l'article 42 du règlement grand-ducal modifié du 21 septembre 1979 concernant les opérations électorales pour la désignation des délégués du personnel, et conformément à l'article 38 du règlement grand-ducal du 24 septembre 1974 concernant les opérations électorales pour la désignation des représentants du personnel dans les comités mixtes d'entreprises et les conseils d'administration des sociétés anonymes, toutes les données à caractère personnel comprises dans les pièces relatives aux élections sont conservées par la délégation du personnel, respectivement par le comité mixte d'entreprise ou par le conseil d'administration, jusqu'à l'expiration du mandat de

la délégation du personnel, du comité mixte ou du conseil d'administration.

Par ailleurs, toutes les données sont susceptibles d'être conservées 5 ans après la fin du mandat de la délégation du personnel, du comité mixte ou du conseil d'administration, lorsque cela s'avère nécessaire pour les besoins de l'entreprise ou de la représentation du personnel concernée.

Participation aux travaux européens

Documents adoptés par le « groupe de travail article 29 » en 2007

Document	Date d'adoption	Référence
Avis commun sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives présentée par la Commission le 6 novembre 2007	05.12.2007	**WP 145**
2e Journée Européenne de la protection de données	05.12.2007	**WP 144**
8th Directive on Statutory Audits, Opinion 10/2007 by the Article 29 Working Party	23.11.2007	**WP 143**
Avis 9/2007 sur le niveau de protection des données à caractère personnel aux îles Féroé	09.10.2007	**WP 142**
Avis 8/2007 sur le niveau de protection des données à caractère personnel à Jersey	09.10.2007	**WP 141**
Avis 7/2007 sur les questions de protection des données liées au système d'information du marché intérieur (IMI)	20.09.2007	**WP 140**
Avis 6/2007 concernant les questions de protection des données posées par le système de coopération en matière de protection des consommateurs (SCPC)	20.09.2007	**WP 139**
Avis 5/2007 concernant le nouvel accord entre l'Union européenne et les Etats-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure, conclu en juillet 2007	17.08.2007	**WP 138**
Rapport 1/2007 sur la première action commune de mise en application : évaluation et étapes à venir	20.06.2007	**WP 137**
Avis nº 4/2007 sur le concept des données à caractère personnel	20.06.2007	**WP 136**
Politique révisée et mise à jour pour promouvoir la transparence des activités du groupe de travail établi par l'article 29 de la directive 95/46/CE	15.02.2007	**WP 135**
Avis n° 3/2007 sur la proposition de règlement du Parlement européen et du Conseil modifiant les instructions consulaires communes adressées aux représentations diplomatiques et consulaires de carrière, en liaison avec l'introduction d'éléments d'identification biométriques et de dispositions relatives à l'organisation de la réception et du traitement des demandes de visa (COM(2006)269 final)	01.03.2007	**WP 134**
Recommandation 1/2007 sur l'application type pour l'approbation des règles d'entreprise contraignantes applicables au transfert des données à caractère personnel	10.01.2007	**WP 133**
Avis 2/2007 concernant l'information des passagers au sujet du transfert des données des dossiers passagers (Passenger Name Record - PNR) aux autorités américaines ANNEXE : Note d'information courte sur les voyages entre l'Union européenne et les Etats-Unis	15.02.2007	**WP 132**
Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)	15.02.2007	**WP 131**
1er Journée Européenne de la protection de données	24.01.2007	**WP 130**
Avis 1/2007 sur le Livre vert sur les technologies de détection dans le travail des services répressifs, des douanes et d'autres services de sécurité	09.01.2007	**WP 129**

« Groupe de travail article 29 » : Programme de travail 2008 - 2009

Mission du groupe de travail

Le groupe de travail a été institué par l'article 29 de la directive 95/46/CE et a pour mission (article 30, paragraphe 1) :

a) d'examiner toute question portant sur la mise en œuvre des dispositions nationales prises en application de ladite directive, en vue de contribuer à leur mise en œuvre homogène ;

b) de donner à la Commission un avis sur le niveau de protection dans la Communauté et dans les pays tiers ;

c) de conseiller la Commission sur tout projet de modification de ladite directive, sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que sur tout autre projet de mesures communautaires ayant une incidence sur ces droits et libertés ; et

d) de donner un avis sur les codes de conduite élaborés au niveau communautaire.

Ces mêmes tâches doivent également être remplies dans le secteur des communications électroniques (article 15, paragraphe 3, de la directive 2002/58/CE).

Activités en 2008-2009

En 2008-2009, sans préjudice des demandes d'avis formulées par la Commission, le groupe de travail a l'intention de se concentrer sur quatre principaux thèmes stratégiques et sur quelques questions d'actualité qu'il estime utile et urgent d'aborder dans le cadre de l'évolution de la protection des données.

Le groupe de travail devra relever trois défis majeurs en 2008-2009, et notamment :

i) les moyens d'améliorer l'impact de la directive 95/46/CE et le rôle du groupe de travail ;

ii) l'impact des nouvelles technologies ;

iii) l'environnement mondial (transferts internationaux de données, respect de la vie privée à l'échelle mondiale et compétences).

Les thèmes abordés seront donc les suivants:

I. Une meilleure mise en œuvre de la directive 95/46/CE

II. La protection des données lors des transferts internationaux

III. La protection des données en rapport avec les nouvelles technologies

IV. Une efficacité accrue du « groupe de travail article 29 »

V. Les questions d'actualité

Ces différents thèmes peuvent être étroitement liés à plusieurs niveaux et le groupe de travail choisira donc le meilleur moyen de les traiter. Ils sont décrits de manière plus détaillée ci-après. Les sujets présentant un plus haut degré de priorité pour le groupe de travail sont marqués d'un astérisque (*).

À intervalles réguliers, le groupe de travail examinera la mise en œuvre de ce programme de travail et il se réserve le droit, le cas échéant, de le préciser davantage ou de le mettre à jour. Il prend également en considération le fait qu'au cours de la période 2008-2009, ce programme de travail sera mis en œuvre dans le cadre de quelque dix réunions plénières et d'environ quarante réunions de sous-groupes.

I. Meilleure mise en œuvre de la directive 95/46/CE

1. Interprétation des dispositions essentielles de la directive 95/46/CE – pour contribuer au projet de communication interprétative[8]

a. «responsable du traitement» et «sous-traitant» (*) – article 2 de la directive 95/46/CE

b. « droit applicable » (*) – article 4 de la directive 95/46/CE

c. « restriction de la finalité » (*) – article 6 de la directive 95/46/CE

d. « raisons du traitement », et notamment le « consentement indubitable » et les « intérêts légitimes » - article 7 de la directive 95/46/CE

2. Instruments d'une mise en œuvre efficace (voir aussi IV)

a. Exécution (*)

8 Dans des documents isolés ou dans des documents thématiques.

b. Expériences nationales - délégués à la protection des données (*)

3. Nouveaux défis

a. Impact du traité modificatif (*)

b. Impact des évolutions technologiques (voir aussi III) et notamment des outils technologiques permettant de garantir la protection

II. La protection des données lors des transferts internationaux

1. Instruments spéciaux

a. Règles d'entreprise contraignantes (BCR) (*)

b. Sphère de sécurité

2. Respect de la vie privée à l'échelle mondiale et compétences

a. Favoriser l'adéquation (*)

b. Normes internationales (meilleure collaboration avec les différents organes normatifs – collaboration active avec ceux qui mettent au point des normes favorisant la prise en compte dès le départ des aspects liés au respect de la vie privée)

c. Droit applicable (voir aussi 1.b)

III. La protection des données en rapport avec les nouvelles technologies

1. Questions liées à l'Internet

a. Moteurs de recherche (*)

b. Réseaux sociaux en ligne (notamment pour les enfants et les adolescents) (*)

c. Établissement des profils de comportement, extraction de données (en ligne ou hors ligne) (*)

d. Radiodiffusion numérique

e. ICANN et WHOIS

2. Réexamen du cadre réglementaire des communications électroniques (*)

3. Gestion de l'identité

4. Administration en ligne

5. Biométrie (utilisation privée et publique – l'accent étant mis sur une application nouvelle ou spécifique de la biométrie) (*)

6. Informatique diffuse (ou ubiquité numérique)

a. Identification par radiofréquence (RFID) (*)

b. Intelligence ambiante

c. Systèmes de télépéage (*)

IV. Accroître l'efficacité du « groupe de travail article 29 »

1. Le rôle du « groupe de travail article 29 » (principes directeurs ou normes directrices pour l'élaboration des avis et la clarification du processus – objectif, priorités, public cible) (*)

2. Amélioration de l'efficacité :

a. Évaluation des documents du groupe de travail en tant qu'instruments pertinents permettant d'uniformiser les pratiques nationales (au niveau du « groupe de travail article 29 ») (*)

b. Échange des meilleures pratiques en matière de contrôle, y compris les expériences récentes en matière de désignation de délégués à la protection des données (au niveau national) (*)

3. Exécution

Identifier les domaines, les secteurs ou les questions suscitant le plus de problèmes (sur la base des informations reçues des autorités chargées de la protection des données) et arrêter des actions communes pertinentes (*)

V. Questions d'actualité

1. Réutilisation des données à des fins de sûreté, et notamment les données relatives aux passagers aériens (données PNR) en Europe (*)

2. Données médicales (dossiers santé en ligne)

3. Archives et vie privée

4. Enfants et vie privée (voir aussi III.1.b) (*)

5. Mise en place d'un cadre pour les audits en matière de respect de la vie privée, destiné aux secteurs privé et public (*outil leur permettant d'évaluer eux-mêmes si les données qu'ils détiennent sont toujours nécessaires, proportionnées, exactes, à jour, etc.*)

6. Aspects financiers

a) SWIFT/SEPA

b) Éventuellement VISA/Mastercard

7. Marketing direct

8. Enquête préalable (*)

« Groupe de travail article 29 » : Liste et composition des sous-groupes 2007

	Pre-Trial Discoveries	Children & Privacy	VISA & Biometrics	Financial Matters	Internet Taskforce (ITF)	Medical Data	Enforcement	Data Transfer to US: - SOX/Safe Harbor	Data Transfer to 3rd Countries: - BCR / COC/ Contractual Clauses	PNR
Austria				X	X	X	X		X	X
Belgium	X	X	X	X	X	X	X			
Bulgaria										
Cyprus										
Czech Republic			X		X					
Denmark					X					
Estonia										
Finland					X					
France	X	X	X	X	X	X		X	X	X
Germany	X	X	X	X	X	X	X	X	X	X
Greece		X				X	X			
Hungary										
Ireland			X	X	X	X				
Italy		X	X	X	X	X	X	X	X	X
Latvia										
Lithuania						X	X			
Luxembourg					X	X		X		
Malta										
Netherlands				X	X	X	X		X	X
Poland			X		X	X	X	X		
Portugal	X	X								
Romania			X	X	X	X	X	X	X	X
Slovakia					X					
Slovenia				X	X					
Spain	X	X		X	X	X	X	X	X	X
Sweden						X				
United Kingdom	X	X	X	X	X		X	X	X	X
EDPS		X		X	X	X				X
Iceland		X								
Liechtenstein										
Norway					X	X				

Documents adoptés par l'« International Working Group on Data Protection in Telecommunication » en 2007

Document	Date d'adoption	Lieu
Working Paper on Privacy Issues in the Distribution of Digital Media Content and Digital Television	04/05.09.2007	Berlin
Working Paper on E-Ticketing in Public Transport	04/05.09.2007	Berlin
Working Paper on Cross-Border Telemarketing	12/13.04.2007	Guernsey

Documents adoptés par le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Document	Date d'adoption	Lieu
Opinion of the T-PD on the interpretation of the concepts of automatic processing and controller of the file in the context of worldwide telecommunications networks	15.03.2007	Strasbourg
Paper outlining the T-PD's initial remarks concerning a proposal for a council framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters	15.03.2007	Strasbourg

Conseil de l'Europe T-PD : Programme de travail pour 2007 et au-delà

1. Status and powers of data protection supervisory authorities

Explanation: The Additional Protocol to Convention 108 foresees the setting up in state parties of independent data protection supervisory authorities, with powers of investigation and intervention, the power to engage in legal proceedings or to bring violations of data protection legislation to the attention of the competent judicial authorities, as well as the power to hear complaints from individuals. However, the concrete status and powers of supervisory authorities vary widely among state parties to Convention 108, even among those that have ratified the Additional Protocol.

Therefore the Bureau thought it a top priority to monitor the situation of data protection authorities in state parties, with a view to proposing adequate measures of implementation of the Additional Protocol.

Action: As a first step, the T-PD and the Bureau will study the status and powers of data protection supervisory authorities in state parties. On this basis, they could then seek to draw up a "model" to accompany the implementation of the Additional Protocol.

2. Role and working methods of the T-PD

Explanation: The steady decrease in the number and length of meetings during the past years make it difficult for the T-PD to carry out all the tasks of its work programme and to react to new developments in the data protection field in a timely manner. Therefore, the T-PD deems necessary to adapt its role and working methods, making best use of its Bureau, in order to maintain its efficiency in a context of budgetary restrictions.

Action: The Bureau will prepare proposals on the role and working methods of the T-PD, possibly involving modifications of the T-PD's internal rules of procedure, that will be considered by the T-PD at its next plenary meeting in 2008. In this connection, the T-PD will also study how to associate the Data Protection Commissioner of the Council of Europe more closely with its work.

3. Fundamental right to data protection

Explanation: At its last plenary meeting, the T-PD entrusted its Bureau with the task of studying the case-law of the European Court of Human Rights, in order to assess the need and added value of a fundamental right to data protection, distinct of article 8 of the ECHR.

In 2006, the Bureau started to analyse the case-law of the Court dealing with data protection, and had an exchange of views on this issue with judge Baka of the European Court of Human Rights.

Action: This work will be pursued in 2007.

4. Data protection issues in the field of police and judicial co-operation

Explanation: The T-PD and its Bureau are following developments of data protection issues in the field of co-operation in police and judicial matters, with a view, if necessary, to determine adequate follow-up. In this framework, the Bureau examined in 2006 the proposal for a framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters.

Action: the T-PD and its Bureau will continue to follow developments in this area in 2007 and adequate action will be proposed as necessary.

5. Opinions on the compatibility with the Council of Europe's data protection instruments

Explanation: In 2006, the Bureau, acting on behalf of the T-PD, prepared at the request of the Secretary General or of other Council of Europe's committees, several opinions on the compatibility of some developments with the Council of Europe's data protection instruments. It proposes to continue and develop this task in 2007 and the following years.

Action: the T-PD and its the Bureau will continue to follow developments within the Council of Europe and outside and opinions will be prepared at the request of other bodies or as necessary.

Data protection matters in the context of global telecommunication networks

6. Profiling

Explanation: At its last plenary meeting, the T-PD decided to commission an expert study on the issue of profiling. Due to unforeseen delays and difficulties, this study will be completed by the end of 2007.

Action: On the basis of the study to be delivered in 2007, the Bureau will propose suitable follow-up to the T-PD plenary meeting in 2008.

7. Transborder data flows: legal framework

Explanation: The ongoing development of telecommunication networks represent a challenge to the current system as laid down in the Additional Protocol and Directive 95/46/EC. A question was also raised as to whether model contracts and binding corporate rules offer sufficient safeguards.

Therefore the Bureau considered it a top priority to think of a combination of legal and technical solutions to surround data transfers with sufficient safeguards. Flexibility is a key aspect, in order for solutions not to become outdated as a result of the rapid evolution of the networks. Provisions of the Lindquist judgment of the Court of Justice of the European Communities and the work of Article 29 Working Party should be kept in mind during work on this issue, as well as the OECD's initiative on cross-border enforcement. The political dimension of this issue (see APIS/PNR case) should not be overlooked either.

Action: A relevant activity on this topic will be proposed once ongoing work at the OECD is completed.

8. Interpretation of the notion of personal data in relation with identity

Explanation: The Bureau felt that the T-PD could work on clarifying the interpretation of the notion of personal data in relation with identity, to allow for new technological and social developments. Notions like temporary identity, anonimysation, categories of data making it possible to piece together a person's identity need to be examined more closely. However, as this is such a vast subject, the Bureau felt it should be advisable to tackle this issue step by step, as the need arises and in connection with other work. Work on this issue would have a bearing on that related to transborder data flows and data processing.

The Article 29 Working Party is currently working on the notion of personal data and identifiability, in the context of its application to new technologies (RFIDs). The T-PD could follow this activity in order to build on its results, but its approach to this issue would be broader.

Action: to be determined in the light of the results of the work of Article 29 Working Party. The T-PD agreed that work on this issue should not be tackled as such, but rather as the need arises, in connection with work on other issues.

B. SECONDARY PRIORITY LEVEL

9. Data protection in the field of employment

Explanation: in the light of the Poullet-Dinant report on the question of data processing within groups (see part II, section 4.4 of the report), the T-PD could carry out a general examination of Recommendation (89) 2 on the protection of personal data used for employment purposes in the light of technological developments and other Council of Europe texts on data protection containing provisions on the processing of data in the employment field, such as the texts on video surveillance, smart cards and biometrics. The purpose of this examination would be to determine whether Recommendation (89) 2 is still up to date and, if necessary, to update it. The work of the ILO, the Berlin Group on data protection in telecommunications and the Article 29 Group could be useful in this connection.

Action: review recent texts issued by the Council of Europe and case-law of the European Court of Human Rights which contain elements relating to data protection in the field of employment, as well as the work of other instances, before determining whether Recommendation (89) 2 needs updating.

As a first step, the Bureau could gather information on concrete examples and cases, following the example of what it is currently doing as a followup of the progress report on biometrics.

10. Review and update of the "older" Recommendations

Action: The T-PD felt it would be useful to carry out a general review and update of other "older" recommendations, but stressed that this would depend on the availability of time and budgetary resources.

Loi modifiée du 2 août 2002

(texte coordonné du 27 juillet 2007)

Texte coordonné de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel modifiée par la loi du 31 juillet 2006, la loi du 22 décembre 2006, la loi du 27 juillet 2007.

Chapitre I. Dispositions générales relatives à la protection de la personne à l'égard des traitements des données à caractère personnel

Art. 1er. Objet

(Loi du 27 juillet 2007)

«La présente loi protège les libertés et les droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel (...).»

Art. 2. Définitions

Aux fins de la présente loi, on entend par :

(a) «*code de conduite*» : contributions sectorielles élaborées en vue de la bonne application de la présente loi. Les codes de conduite sont élaborés à l'échelon national ou communautaire par les associations professionnelles et les autres organisations représentatives des responsables du traitement et sont facultativement soumis pour approbation à la Commission nationale ou au groupe de protection des personnes à l'égard du traitement des données à caractère personnel tel qu'institué par l'article 29 de la Directive 95/46/CE ;

(b) «*Commission nationale*» : la Commission nationale pour la protection des données ;

(Loi du 27 juillet 2007)

«(c) «*consentement de la personne concernée*» : toute manifestation de volonté (…) libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou statutaire accepte que les données à caractère personnel fassent l'objet d'un traitement ;»

(d) «*destinataire*» : 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; les autorités qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre de l'exécution d'une mission légale d'enquête ou de contrôle ne sont pas considérées comme des destinataires ;

(Loi du 27 juillet 2007)

«(e) «*donnée à caractère personnel*» (ci-après dénommée «donnée») : 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 (…) 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 ;»

(f) «*donnée relative à la santé*» : toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques ;

(g) «*donnée génétique*» : toute donnée concernant les caractères héréditaires d'un individu ou d'un groupe d'individus apparentés ;

(h) «*fichier de données à caractère personnel*» (ci-après dénommé «fichier») : tout ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;

(i) «*instance médicale*» : tout praticien de la santé et toute personne soumise à la même obligation de secret professionnel, ainsi que tout établissement hospitalier visé par la loi du 28 août 1998 sur les établissements hospitaliers, effectuant un traitement de données nécessaire aux fins de la médecine préventive, des diagnostics

médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé ; «*interconnexion*» *: est abrogée par la loi du 27 juillet 2007*

(j) «*ministre*» : le ministre ayant dans ses attributions la protection des données ;

(Loi du 22 décembre 2006)

(k) «*organisme de sécurité sociale*» : tout organisme de droit public ou privé qui assure des prestations, obligatoires ou facultatives, relatives à la maladie, la maternité, la vieillesse, les accidents corporels, l'invalidité, la dépendance, le décès, le chômage, «le congé parental» ainsi que des prestations familiales ou d'aides sociales ;

(l) «*pays tiers*» : Etat non membre de l'Union européenne ;

2339

(Loi du 27 juillet 2007.)

«(m) «*personne concernée*» : toute personne physique (…) qui fait l'objet d'un traitement de données à caractère personnel ;»

(n) «*responsable du traitement*» : 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 ;

(o) «*sous-traitant*» : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données pour le compte du responsable du traitement ;

(Loi du 27 juillet 2007)

«(p) «*surveillance*» : toute activité qui, opérée au moyen d'instruments techniques, consiste en l'observation, la collecte ou l'enregistrement de manière non occasionnelle des données à caractère personnel d'une ou de plusieurs personnes, relatives à des comportements, des mouvements, des communications ou à l'utilisation d'appareils électroniques et informatisés ;»

(q) «*tiers*» : 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. Dans le secteur public, on entend par tiers un ministère, une administration, un établissement public, une commune ou un service public autre que le responsable du traitement ou son sous-traitant ;

(r) «*traitement de données à caractère personnel*» (ci-après dénommé «traitement») : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Art. 3. Champ d'application

(Loi du 27 juillet 2007)

«(1) La présente loi s'applique :

- au traitement automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données contenues ou appelées à figurer dans un fichier ;

- à toute forme de captage, de traitement et de diffusion de sons et images qui permettent d'identifier des personnes physiques ;

- au traitement 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.

(2) Est soumis à la présente loi :

(a) le traitement mis en oeuvre par un responsable du traitement établi sur le territoire luxembourgeois ;

(b) le traitement mis en œuvre par un responsable du traitement qui, sans être établi sur le territoire luxembourgeois ou sur celui d'un autre Etat membre de l'Union européenne, recourt à des moyens de traitement situés sur le territoire luxembourgeois, à l'exclusion des moyens qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de l'Union européenne.

Pour le traitement mentionné à l'article 3, paragraphe (2) lettre (b), le responsable du traitement désigne par une déclaration écrite à la Commission nationale un représentant établi sur le territoire luxembourgeois qui se substitue au responsable du traitement dans l'accomplissement de ses obligations prévues par la présente loi sans que ce dernier ne soit dégagé de sa propre responsabilité.

(3) La présente loi ne s'applique pas au traitement mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques.»

Chapitre II. Conditions de licéité du traitement

Art. 4. Qualité des données

(1) 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 sans préjudice du paragraphe (2) ci-après.

(Loi du 27 juillet 2007)

«(2) 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 collectées.»

(3) Quiconque effectue un traitement en violation des dispositions du présent article 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 5. Légitimité du traitement

(Loi du 27 juillet 2007)

«(1) Le traitement de données ne peut être effectué que (...) :

(a) s'il (…) est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou

(b) s'il (…) 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 ou les tiers auxquels les données sont communiquées, ou

(c) s'il (…) est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci, ou

(d) s'il (…) 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, ou

(e) s'il (…) est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou

(f) si la personne concernée a donné son consentement.»

(2) Quiconque effectue un traitement en violation des dispositions du présent article 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 6. Traitement de catégories particulières de données

(1) Les traitements qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les traitements de données relatives à la santé et à la vie sexuelle, y compris le traitement des données génétiques sont interdits.

(2) Le paragraphe (1) ne s'applique pas lorsque :

(*Loi du 27 juillet 2007*)

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

(Loi du 27 juillet 2007)

(b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement (…) en matière de droit du travail dans la mesure où il est autorisé par la loi, ou lorsque

(c) 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'incapacité physique ou juridique de donner son consentement, ou lorsque

(d) le traitement est mis en œuvre, avec le consentement de la personne concernée par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, dans le cadre de leurs activités légitimes, à condition que le traitement se rapporte aux données nécessaires des seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées, ou lorsque

(e) le traitement porte sur des données manifestement rendues publiques par la personne concernée, ou lorsque

(Loi du 27 juillet 2007)

«(f) le traitement (…) est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice(…), ou lorsque

(g) le traitement s'avère nécessaire pour un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques sans préjudice de l'application de l'article 7 ci-après (…), ou lorsque»

(h) le traitement est mis en œuvre par voie de règlement grand-ducal tel que prévu à l'article 17, «ou lorsque»

(Loi du 27 juillet 2007)

«(i) le traitement est mis en œuvre dans le cadre

d'un traitement de données judiciaires au sens de l'article 8. (…)

(3) Toutefois, (…) les données génétiques ne peuvent faire l'objet d'un traitement que :

a) pour vérifier l'existence d'un lien génétique dans le cadre de l'administration de la preuve en justice, pour l'identification d'une personne, la prévention ou la répression d'une infraction pénale déterminée dans les cas visés au paragraphe (2) du présent article par les lettres (f), (h) et (i), ou

b) dans le cas visé au paragraphe (2) du présent article par la lettre (c) lorsque le traitement est nécessaire à la sauvegarde des intérêts vitaux, ou

c) dans le cas visé au paragraphe (2) du présent article par la lettre (g) lorsque le traitement s'avère nécessaire pour un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques, ou

d) dans le cas visé à l'article 7, paragraphe (2) lorsque la personne concernée a donné son consentement exprès et si le traitement est effectué dans les seuls domaines de la recherche en matière de santé ou de la recherche scientifique sauf indisponibilité du corps humain et sauf dans le cas où la loi prévoit que l'interdiction visée au paragraphe

(1) ne peut être levée par le consentement de la personne concernée.

Dans les cas où la loi permet la levée de l'interdiction par le consentement de la personne concernée, mais qu'il s'avère que pour des raisons pratiques le consentement est impossible à requérir ou disproportionné par rapport à l'objectif recherché et sans préjudice du droit d'opposition de la personne concernée, il peut être passé outre à l'exigence du consentement préalable dans des conditions à déterminer par règlement grand-ducal, ou

e) dans le cas visé à l'article 7, paragraphe (1), lorsque le traitement de données génétiques est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, ou de l'administration de soins ou de traitements. Dans ce cas, le traitement de ces données ne peut être mis en œuvre que par les instances médicales.»

(4) Quiconque effectue un traitement ou opère une communication à un tiers en violation des dispositions du paragraphe (1) qui précède 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. La juridiction saisie peut prononcer la cessation du traitement ou de la communication contraires aux dispositions du paragraphe (1) du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 7. Traitement de catégories particulières de données par les services de la santé

(Loi du 27 juillet 2007)

«Sans préjudice de l'application de l'article 6 paragraphe (3) relatif au traitement des données génétiques :

(1) le traitement de données relatives à la santé et à la vie sexuelle nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements peut être mis en œuvre par des instances médicales ;

(2) le traitement de données relatives à la santé et à la vie sexuelle nécessaire aux fins de la recherche en matière de santé ou de la recherche scientifique peut être mis en œuvre par des instances médicales, ainsi que par les organismes de recherche et par les personnes physiques ou morales dont le projet de recherche a été approuvé en vertu de la législation applicable en matière de recherche biomédicale. Si le responsable est une personne morale, il indique un responsable délégué soumis au secret professionnel ;

(3) le traitement de données relatives à la santé et à la vie sexuelle nécessaire aux fins de la gestion de services de santé peut être mis en œuvre par des instances médicales, ainsi que lorsque le responsable du traitement est soumis au secret professionnel, par les organismes de sécurité sociale et les administrations qui gèrent ces données en exécution de leurs missions légales et réglementaires, par les entreprises d'assurance, les

sociétés gérant les fonds de pension, la Caisse médico-chirurgicale mutualiste et par celles des personnes physiques ou morales bénéficiant d'un agrément dans le domaine médico-social ou thérapeutique en vertu de la loi du 8 septembre 1998 réglant les relations entre l'Etat et les organismes œuvrant dans les domaines social, familial et thérapeutique lorsqu'ils développent leur activité dans l'un des domaines à énumérer par règlement grand-ducal.

(4) Le recours à un sous-traitant est possible dans les conditions prévues à l'article 21.

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.

Les prestataires de soins et les fournisseurs peuvent communiquer les données relatives à leurs prestations au médecin traitant et à un organisme de sécurité sociale ou à la Caisse médico-chirurgicale mutualiste aux fins de remboursement des dépenses afférentes.

(5) Quiconque effectue un traitement ou opère une communication à un tiers en violation des dispositions du présent article 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. La juridiction saisie peut prononcer la cessation du traitement ou de la communication contraires aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.»

Art. 8. Traitement de données judiciaires

(1) Le traitement des données dans le cadre d'enquêtes pénales et de procédures judiciaires est opéré dans le respect des dispositions du Code d'instruction criminelle, du Code de procédure civile, de la loi portant règlement de procédure devant les juridictions administratives ou d'autres lois.

(2) 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.

(3) Il ne peut être tenu de recueil exhaustif des condamnations pénales que sous le contrôle de l'autorité publique compétente en la matière.

(4) Quiconque, agissant à titre privé, effectue un traitement en violation des dispositions du présent article 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 9. Traitement réalisé dans le cadre de la liberté d'expression

(*Loi du 27 juillet 2007*)

(...) Sans préjudice des dispositions prévues dans la «loi du 8 juin 2004 sur la liberté d'expression dansles médias» et dans la mesure où les dérogations ci-après s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression, le traitement mis en œuvre aux seules fins de journalisme ou d'expression artistique ou littéraire n'est pas soumis :

(a) - à la prohibition de traiter les catégories particulières de données telle que prévue à l'article 6, paragraphe (1) ;

- aux limitations concernant le traitement de données judiciaires prévues à l'article 8 ;

(Loi du 27 juillet 2007) « lorsque le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou à des données qui sont en rapport direct avec la vie publique de la personne concernée ou avec le fait dans lequel elle est impliquée de façon volontaire ;»

(b) à la condition de protection adéquate exigée s'agissant des traitements de données faisant l'objet d'un transfert vers un pays tiers telle que prévue à l'article 18, paragraphe (1) ;

(c) à l'obligation d'information de l'article 26, paragraphe (1), lorsque son application compromettrait la collecte des données auprès de la personne concernée ;

(d) à l'obligation d'information de l'article 26, paragraphe (2), lorsque son application compromettrait soit la collecte des données, soit une publication en projet, soit la mise à disposition du public, de quelque manière que ce soit de ces données ou fournirait des indications permettant d'identifier les sources d'information ;

(Loi du 27 juillet 2007)

«(e) au droit d'accès de la personne concernée qui est différé et limité conformément (…) à l'article 29, paragraphe (3).»

(…)

Art. 10. Traitement à des fins de surveillance

(1) Le traitement à des fins de surveillance ne peut être effectué que :

(a) si la personne concernée a donné son consentement, ou

(b) aux abords ou dans tout lieu accessible ou non au public autres que les locaux d'habitation, notamment dans les parkings couverts, les gares, aérogares et les moyens de transports publics, pourvu que le lieu en question présente de par sa nature, sa situation, sa configuration ou sa fréquentation un risque rendant le traitement nécessaire :

(Loi du 27 juillet 2007)

«-à la sécurité des usagers ainsi qu'à la prévention des accidents ;(…)

-à la protection des biens, s'il existe un risque caractérisé de vol ou de vandalisme», ou

(c) aux lieux d'accès privé dont la personne physique ou morale y domiciliée est le responsable du traitement, «ou»

(Loi du 27 juillet 2007)

«(d) si 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'incapacité physique ou juridique de donner son consentement.»

(2) Les personnes concernées sont informées par des moyens appropriés tels que des panneaux de signalisation, des circulaires et/ou des envois recommandés par voie postale ou électronique de la mise en œuvre des traitements visés au paragraphe (1), lettres (b) et (c). A la demande de la personne concernée, le responsable du traitement fournit à celle-ci les informations prévues à l'article 26, paragraphe (2).

(3) Les données collectées à des fins de surveillance ne sont communiquées que :

(a) si la personne concernée a donné son consentement sauf le cas interdit par la loi, ou

(b) aux autorités publiques dans le cadre de l'article 17, paragraphe (1), ou

(c) aux autorités judiciaires compétentes pour constater ou poursuivre une infraction pénale et aux autorités judiciaires devant lesquelles un droit en justice est exercé ou défendu.

(4) Quiconque effectue un traitement en violation des dispositions du paragraphe (1) qui précède 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du paragraphe (1) du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 11. *Abrogé par la loi du 31 juillet 2006 et repris par l'article L. 261-1 Code du Travail*

(Loi du 27 juillet 2007)

«Art. 11 nouveau : Traitement à des fins de surveillance sur le lieu de travail

Le traitement à des fins de surveillance sur le lieu de travail ne peut être mis en œuvre par l'employeur, s'il est le responsable du traitement, que dans les

conditions visées à l'article L. 261-1 du Code du Travail.»

Chapitre III. Formalités préalables à la mise en œuvre des traitements et publicités des traitements

Art. 12. Notification préalable à la Commission nationale

(1) (a) A l'exception de ceux qui relèvent des dispositions prévues aux articles 8, 14 et 17, les traitements de données font l'objet d'une notification préalable par le responsable du traitement auprès de la Commission nationale.

(b) Les traitements relevant d'un même responsable du traitement et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une notification unique. Dans ce cas les informations requises en application de l'article 13 ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

(Loi du 27 juillet 2007)

«(2) Sont exemptés de l'obligation de notification :

(a) les traitements, sauf ceux à des fins de surveillance visés aux articles 10 ci-dessus et L. 261-1 du Code du Travail, effectués par le responsable du traitement, s'il désigne un chargé de la protection des données. Le chargé de la protection des données établit et continue à la Commission nationale un registre comprenant les traitements effectués par le responsable du traitement, à l'exception de ceux exemptés de notification conformément au paragraphe (3) du présent article et conformément aux dispositions relatives à la publicité des traitements telles que prévues à l'article 15 ;

(b) les traitements ayant pour seul but la tenue d'un registre qui en vertu d'une disposition légale est destiné à l'information du public et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime ;

(c) les traitements mis en œuvre par les avocats, notaires et huissiers, et nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;

(d) les traitements mis en œuvre aux seules fins de journalisme ou d'expression artistique ou littéraire visés à l'article 9 ;

(e) les traitements nécessaires 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'incapacité physique ou juridique de donner son consentement.

(3) Sont en outre exemptés de l'obligation de notification :

(a) Les traitements de données qui se rapportent exclusivement à des données à caractère personnel nécessaires à l'administration des salaires des personnes au service ou travaillant pour le responsable du traitement, pour autant que ces données soient utilisées exclusivement pour l'administration des salaires visée et qu'elles soient uniquement communiquées aux destinataires qui y ont droit.

(b) Les traitements de données qui visent exclusivement la gestion des candidatures et des recrutements ainsi que l'administration du personnel au service ou travaillant pour le responsable du traitement.

Le traitement ne peut se rapporter ni à des données relatives à la santé de la personne concernée, ni à des données sensibles ou judiciaires au sens des articles 6 et 8, ni à des données destinées à une évaluation de la personne concernée.

Ces données ne peuvent être communiquées à des tiers, sauf dans le cadre de l'application d'une disposition légale ou réglementaire, ou pour autant qu'elles soient indispensables à la réalisation des objectifs du traitement.

(c) Les traitements de données qui se rapportent exclusivement à la comptabilité du responsable du traitement, pour autant que ces données soient utilisées exclusivement pour cette comptabilité et que le traitement concerne uniquement des personnes dont les données sont nécessaires à la comptabilité.

Ces données ne peuvent être communiquées à des tiers, sauf dans le cadre de l'application d'une disposition réglementaire ou légale ou pour autant que la communication soit indispensable pour la comptabilité.

(d) Les traitements de données qui visent exclusivement l'administration d'actionnaires, d'obligataires et d'associés, pour autant que le traitement porte uniquement sur les données nécessaires à cette administration, que ces données portent uniquement sur des personnes dont les données sont nécessaires à cette administration, que ces données ne soient pas communiquées à des tiers, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

(e) Les traitements de données qui visent exclusivement la gestion de la clientèle ou des fournisseurs du responsable du traitement.

Le traitement peut uniquement porter sur des clients ou des fournisseurs potentiels, existants ou anciens du responsable du traitement.

Le traitement ne peut se rapporter ni à des données relatives à la santé de la personne concernée, ni à des données sensibles ou judiciaires au sens des articles 6 et 8.

Ces données ne peuvent être communiquées à des tiers, sauf dans le cadre de l'application d'une disposition légale ou réglementaire, ou encore aux fins de la gestion normale d'entreprise.

(f) Les traitements de données qui sont effectués par une fondation, une association ou tout autre organisme sans but lucratif dans le cadre de leurs activités ordinaires.

Le traitement doit se rapporter exclusivement à l'administration des membres propres, des personnes avec qui le responsable du traitement entretient des contacts réguliers ou des bienfaiteurs de la fondation, de l'association ou de l'organisme.

Ces données ne peuvent être communiquées à des tiers, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

(g) Les traitements de données d'identification indispensables à la communication effectués dans le seul but d'entrer en contact avec l'intéressé, pour autant que ces données ne soient pas communiquées à un tiers.

La lettre (g) s'applique uniquement aux traitements de données non visés par une des autres dispositions de la présente loi.

(h) Les traitements de données portant exclusivement sur l'enregistrement de visiteurs, effectué dans le cadre d'un contrôle d'accès manuel, dans la mesure où les données traitées se limitent aux seuls nom, adresse professionnelle du visiteur, identification de son employeur, identification de son véhicule, nom, section et fonction de la personne visitée ainsi qu'au jour et à l'heure de la visite.

Ces données ne peuvent être utilisées exclusivement que pour le contrôle d'accès manuel.

(i) Les traitements de données qui sont effectués par les établissements d'enseignement en vue de gérer leurs relations avec leurs élèves ou étudiants.

Le traitement se rapporte exclusivement à des données à caractère personnel relatives à des élèves ou étudiants potentiels, actuels ou anciens de l'établissement d'enseignement concerné.

Ces données ne peuvent être communiquées à des tiers, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

(j) Les traitements de données à caractère personnel effectués par des autorités administratives si le traitement est soumis à des réglementations particulières adoptées par ou en vertu de la loi et réglementant l'accès aux données traitées ainsi que leur utilisation et leur obtention.

(k) Les traitements de données à caractère personnel nécessaires à la gestion des systèmes et réseaux informatiques et de communications électroniques, pourvu qu'ils ne soient pas mis en œuvre à des fins de surveillance au sens des articles 10 et 11 nouveau.

(l) Les traitements mis en œuvre conformément à l'article 36 de la loi du 28 août 1998 sur les établissements hospitaliers à l'exception des traitements de données génétiques.

(m) Les traitements mis en œuvre conformément à l'article 7 paragraphe (1) par un médecin et concernant ses patients à l'exception des traitements de données génétiques.

(n) Les traitements mis en œuvre par un pharmacien et par un professionnel soumis à la loi modifiée du 26 mars 1992 sur l'exercice et la revalorisation de certaines professions de santé. Le traitement de données à caractère personnel se rapporte exclusivement à la délivrance des médicaments et aux soins ou prestations effectuées. Ces données ne peuvent être communiquées à des tiers, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.»

(4) Quiconque ne se soumet pas à l'obligation de notification ou fournit des informations incomplètes ou inexactes est puni d'une amende de 251 à 125.000 euros. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 13. Contenu et forme de la notification

(1) La notification comprend au moins les informations suivantes :

(Loi du 27 juillet 2007.)

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

(b) la condition de légitimité du traitement ;

(c) la ou les finalité(s) du traitement ;

(d) la description de la ou des catégories de personnes concernées et des données ou des catégories de données s'y rapportant ;

(e) les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées ;

(f) les pays tiers à destination desquels des transferts de données sont envisagés ;

(g) une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement en application des articles 22 et 23 ;

(…) abrogée par la loi du 27 juillet 2007

(2) Toute modification affectant les informations visées au paragraphe (1) doit être notifiée à la Commission nationale préalablement à la mise en œuvre du traitement.

(Loi du 27 juillet 2007)

«(3) La notification se fait auprès de la Commission nationale moyennant support papier accompagné, le cas échéant, d'un support informatique ou d'une transmission par voie électronique suivant un schéma à établir par elle. Il est accusé réception de la notification.

Un règlement grand-ducal fixe le montant et les modalités de paiement d'une redevance à percevoir lors de toute notification et de toute modification de notification.

(4) Les traitements qui ont une même finalité, qui portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent faire l'objet d'une notification unique auprès de la Commission nationale. Dans ce cas le responsable de chaque traitement adresse à la Commission nationale un engagement formel de conformité de celui-ci à la description figurant dans la notification.»

Art. 14. Autorisation préalable de la Commission nationale

(Loi du 27 juillet 2007)

«(1) Sont soumis à l'autorisation préalable de la Commission nationale :

(a) les traitements de données génétiques visés au paragraphe (3) lettres (c) et (d) de l'article 6 ;

(b) les traitements à des fins de surveillance visés à l'article 10 dès lors que les données résultant de la surveillance font l'objet d'un enregistrement et à l'article 11 nouveau ;

(c) les traitements de données à des fins historiques, statistiques ou scientifiques visés à l'article 4,paragraphe (2) ;

(d) l'interconnexion de données visée à l'article 16 ;

(e) le traitement concernant le crédit et la solvabilité des personnes concernées lorsque ce traitement est effectué par des personnes autres que des professionnels du secteur financier ou des compagnies d'assurance concernant leurs clients ;

(f) les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes ;

(g) l'utilisation de données à des fins autres que celles pour lesquelles elles ont été collectées. Un tel traitement ne peut être effectué que moyennant consentement préalable de la personne concernée ou s'il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée.»

(2) La demande d'autorisation comprend les informations suivantes :

(Loi du 27 juillet 2007)

(a) le nom et l'adresse du responsable du traitement (…) «et le cas échéant» de son représentant (…) ;

(b) la condition de légitimité du traitement ;

(c) la ou les finalités du traitement ;

(d) l'origine des données ;

(e) la description détaillée des données ou catégories de données ainsi que des traitements envisagés ;

(f) la description de la ou des catégories de personnes concernées ;

(g) les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées ;

(h) les pays tiers à destination desquels des transferts de données sont envisagés ;

(i) une description détaillée permettant d'apprécier le respect des mesures de sécurité prévues auxarticles 22 et 23.

(…) abrogée par la loi du 27 juillet 2007

(Loi du 27 juillet 2007)

«(3) Toute modification affectant les informations visées au paragraphe (2) doit être autorisée par la Commission nationale préalablement à la mise en œuvre du traitement.

(4) La demande d'autorisation se fait auprès de la Commission nationale moyennant support papier accompagné, le cas échéant, d'un support informatique ou d'une transmission par voie électronique. Il est accusé réception de la demande d'autorisation. Un règlement grand-ducal fixera le montant et les modalités de paiement d'une redevance à percevoir lors de toute autorisation et de toute modification d'autorisation.»

(5) Les traitements qui ont une même finalité, qui portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisées par une décision unique de la Commission nationale. Dans ce cas le responsable de chaque traitement adresse à la Commission nationale un engagement formel de conformité de celui-ci à la description figurant dans l'autorisation.

(6) Quiconque effectue un traitement en violation des dispositions du présent article 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 15. Publicité des traitements

(1) La Commission nationale tient un registre public des traitements.

(2) Figurent dans ce registre :

(a) les traitements notifiés à la Commission nationale en vertu de l'article 12, paragraphe (1) ;

(b) les traitements autorisés par la Commission nationale en vertu de l'article 14, paragraphe (1) ; et

(Loi du 27 juillet 2007)

«(c) les traitements surveillés par le chargé de la protection des données et continués à la Commission nationale en vertu de l'article 12, paragraphe (2) lettre (a) ainsi que l'identité de celui-ci.»

(3) Le registre tenu par la Commission nationale contient sur chaque traitement les informations requises respectivement par l'article 13, paragraphe (1) et par l'article 14, paragraphe (2). Pour les traitements soumis à autorisation préalable, le registre renseigne en plus sur l'autorisation émise par la Commission nationale.

(4) Toute personne peut prendre connaissance, et ce gratuitement, des informations contenues dans le registre public qui est en ligne, à l'exception de celles prévues respectivement à l'article 13, paragraphe (1) lettre (g) et à l'article 14, paragraphe (2) lettre (i).

(5) Cependant la Commission nationale peut limiter cette publicité lorsqu'une telle mesure est nécessaire pour sauvegarder :

(a) la sûreté de l'Etat,

(b) la défense,

(c) la sécurité publique,

(Loi du 27 juillet 2007)

«(d) la prévention, la recherche et la constatation d'infractions pénales et la lutte contre le blanchiment,»

(e) un intérêt économique ou financier important de l'Etat ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal,

(f) la protection de la personne concernée ou des droits et libertés d'autrui,

(g) la liberté d'expression,

(h) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points (c), (d) et (e) et

(i) le secret professionnel et le secret d'affaires de la personne concernée et du responsable du traitement.

(6) La Commission nationale publie un rapport annuel qui fait état des notifications et autorisations.

(7) Le présent article ne s'applique pas aux traitements ayant pour seul but la tenue d'un registre qui, en vertu d'une loi ou d'un règlement grand-ducal, est destiné à l'information du public et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

Art. 16. Interconnexion de données

(Loi du 27 juillet 2007)

(1) L'interconnexion de données qui n'est pas expressément prévue par un texte légal «ou réglementaire» doit faire l'objet d'une autorisation préalable de la Commission nationale sur demande conjointe présentée par les responsables des traitements en cause.

(2) L'interconnexion de données doit permettre d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements, ne pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées, être assortie de mesures de sécurité appropriées et tenir compte du type de données faisant l'objet de l'interconnexion.

(Loi du 27 juillet 2007)

«(3) L'interconnexion n'est autorisée que dans le respect des finalités compatibles entre elles de fichiers et du respect du secret professionnel auquel les responsables du traitement sont le cas échéant astreints.»

Art. 17. Autorisation par voie réglementaire

(1) Font l'objet d'un règlement grand-ducal :

(a) 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,

(b) les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique, et

(c) 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),

(Loi du 27 juillet 2007)

«(d) la création et l'exploitation, aux fins et conditions visées sous (a), d'un système de vidéosurveillance des zones de sécurité. Est à considérer comme telle tout lieu accessible au public qui par sa nature, sa situation, sa configuration ou sa fréquentation présente un risque accru d'accomplissement d'infractions pénales. Les zones de sécurité sont fixées dans les conditions prévues par règlement grand-ducal.»

(2) Le contrôle et la surveillance des traitements mis en œuvre tant en application d'une disposition de droit interne qu'en application d'une convention internationale est exercé par une autorité de contrôle composée du Procureur Général d'Etat, ou de son délégué qui la préside, et de deux membres de la Commission nationale nommés, sur proposition de celle-ci, par le ministre.

L'organisation et le fonctionnement de l'autorité de contrôle font l'objet d'un règlement grand-ducal.

L'autorité de contrôle est informée immédiatement de la mise en œuvre d'un traitement de données visé par le présent article. Elle veille à ce que ces traitements soient effectués conformément aux dispositions légales qui les régissent.

Pour l'exercice de sa mission, l'autorité de contrôle a un accès direct aux données traitées. Elle peut procéder, quant aux traitements effectués, à des vérifications sur place et se faire communiquer tous renseignements et documents utiles à sa mission.

Elle peut également charger un de ses membres à procéder à des missions de contrôle spécifique qui sont exécutées dans les conditions indiquées cidessus.

L'autorité de contrôle fait opérer les rectifications et radiations nécessaires. Elle présente chaque année au ministre un rapport rendant compte de l'exécution de sa mission.

Le droit d'accès aux données visées au présent article ne peut être exercé que par l'intermédiaire de l'autorité de contrôle. Celle-ci procède aux vérifications et investigations utiles, fait opérer les rectifications nécessaires et informe la personne concernée que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exécution.

(3) Toute personne, agissant à titre privé, qui effectue un traitement en violation des dispositions du présent article est punie 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Chapitre IV. Transferts de données vers des pays tiers

Art. 18. Principes

(1) 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.

(2) Le caractère adéquat du niveau de protection offert par un pays tiers doit être apprécié par le responsable du traitement au regard de toutes les circonstances relatives à un transfert ou une catégorie de transferts de données, notamment la nature des données, la finalité et la durée du ou des traitements envisagés, le pays d'origine et le pays de destination finale, les règles de droit générales et sectorielles en vigueur dans le pays en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.

(3) En cas de doute, le responsable du traitement informe sans délai la Commission nationale qui apprécie si un pays tiers assure un niveau de protection adéquat. La Commission nationale notifie conformément à l'article 20 à la Commission européenne les cas dans lesquels elle estime que le pays tiers n'assure pas un niveau de protection adéquat.

(4) Lorsque la Commission européenne ou la Commission nationale constate qu'un pays tiers ne dispose pas d'un niveau de protection adéquat, tout transfert de données vers ce pays est prohibé.

(5) Quiconque effectue un transfert de données vers un pays tiers en violation des dispositions des paragraphes (1), (2) et (4) qui précèdent 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. La juridiction saisie peut prononcer la cessation du transfert contraire aux dispositions des paragraphes (1), (2) et (4) du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 19. Dérogations

(1) Le transfert de données ou d'une catégorie de données vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 18, paragraphe (2), peut toutefois être effectué à condition que :

(a) la personne concernée ait donné son consentement au transfert envisagé, ou

(b) le transfert soit nécessaire à l'exécution d'un contrat auquel la personne concernée et le responsable du traitement sont parties ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée, ou

(c) le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers, ou

(d) le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice, ou

(e) le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou

(Loi du 27 juillet 2007)

(f) le transfert intervienne depuis un registre public tel que prévu à l' «article 12 paragraphe (2) lettre (b).»

(Loi du 27 juillet 2007)

«(2) Dans le cas d'un transfert effectué vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 18, paragraphe (2), le responsable du traitement doit, sur demande de la Commission nationale, notifier à celle-ci, endéans la quinzaine de la demande, un rapport établissant les conditionsdans lesquelles il a opéré le transfert.»

(3) Sans préjudice des dispositions du paragraphe (1), la Commission nationale peut autoriser, sur la base d'une demande dûment motivée, un transfert ou un ensemble de transferts de données vers un pays tiers et n'assurant pas un niveau de protection adéquat, au sens de l'article 18, paragraphe (2), ceci lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes concernées, ainsi qu'à l'exercice des droits correspondants. Ces garanties peuvent résulter de clauses contractuelles appropriées. Le responsable du

traitement est tenu de se conformer à la décision de la Commission nationale.

(4) Quiconque effectue un transfert de données vers un pays tiers en violation des dispositions du présent article 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. La juridiction saisie peut prononcer la cessation du transfert contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 20. Information réciproque

(Loi du 27 juillet 2007)

«(1) La Commission nationale informe le ministre de toute décision prise en application des articles 18, paragraphes (3) et (4), et 19, paragraphe (3).»

(2) Le ministre informe la Commission nationale de toute décision relative au niveau de protection d'un pays tiers prise par la Commission européenne.

Chapitre V. Subordination et sécurité des traitements

Art. 21. Subordination

Toute personne qui agit sous l'autorité du responsable du traitement ou sous celle du sous-traitant, ainsi que le sous-traitant lui-même, et qui accède à des données ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales.

Art. 22. Sécurité des traitements

(Loi du 27 juillet 2007)

(1) 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. «Une description de ces mesures ainsi que de tout changement ultérieur majeur est, à sa demande et dans les quinze jours, communiquée à la Commission nationale.»

(2) Lorsque le traitement est mis en œuvre pour compte du responsable du traitement, celui-ci doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect de ces mesures.

(3) Tout traitement effectué pour compte doit être régi par un contrat ou un acte juridique consigné par écrit qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que :

(a) le sous-traitant n'agit que sur la seule instruction du responsable du traitement ; et que

(b) les obligations visées au présent article incombent également à celui-ci.

Art. 23. Mesures de sécurité particulières

En fonction du risque d'atteinte à la vie privée, ainsi que de l'état de l'art et des coûts liés à leur mise en œuvre, les mesures visées à l'article 22, paragraphe (1) doivent :

(a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données (contrôle à l'entrée des installations) ;

(b) empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée (contrôle des supports) ;

(c) empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées (contrôle de la mémoire) ;

(d) empêcher que des systèmes de traitements de données puissent être utilisés par des personnes non autorisées à l'aide d'installations

de transmission de données (contrôle de l'utilisation) ;

(e) garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur compétence (contrôle de l'accès) ;

(f) garantir que puisse être vérifié et constaté l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission (contrôle de la transmission) ;

(g) garantir que puisse être vérifié et constaté a posteriori l'identité des personnes ayant eu accès au système d'information et quelles données ont été introduites dans le système, à quel moment et par quelle personne (contrôle de l'introduction) ;

(h) empêcher que, lors de la communication de données et du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport) ;

(i) sauvegarder les données par la constitution de copies de sécurité (contrôle de la disponibilité).

Art. 24. Secret professionnel

(1) Les membres de la Commission nationale et toute personne qui exerce des fonctions auprès de la Commission nationale ou accomplit une mission pour son compte ainsi que le chargé de la protection des données sont soumis au respect du secret professionnel prévu à l'article 458 du Code pénal, même après la fin de leur fonction.

(2) Le chargé de la protection des données agissant dans le cadre de l'accomplissement de ses missions, ne peut opposer à la Commission nationale le secret professionnel auquel il est soumis.

(3) Le prestataire de service de certification ne peut opposer à la Commission nationale le secret professionnel auquel il est soumis conformément à l'article 19 de la loi du 14 août 2000 relative au commerce électronique.

(Loi du 27 juillet 2007)

(4) Le responsable du traitement agissant dans le cadre de l'accomplissement de ses missions visées à l'article 7, «paragraphes (1er) et (2)», ne peut opposer à la Commission nationale le secret professionnel auquel il est soumis lorsque celle-ci a été saisie conformément à l'article 32, paragraphes (4) et (5).

Art. 25. Sanctions relatives à la subordination et à la sécurité des traitements

Quiconque effectue un traitement en violation des règles relatives à la confidentialité ou à la sécurité visées aux articles 21, 22 et 23 est puni d'un emprisonnement de huit jours à six mois et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions des articles 21, 22 et 23 sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Chapitre VI. Droits de la personne concernée

Art. 26. Le droit à l'information de la personne concernée

(1) Lorsque des données sont collectées directement auprès de la personne concernée, le responsable du traitement doit fournir à la personne concernée, au plus tard lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes, sauf si la personne concernée en a déjà été informée :

(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 ;

(…) abrogée par la loi du 27 juillet 2007

(Loi du 27 juillet 2007)

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

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

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

(c) toute information supplémentaire telle que :

- les catégories de données concernées ;

- les destinataires ou les catégories de destinataires 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 ;

(…) abrogée par la loi du 27 juillet 2007

(Loi du 27 juillet 2007)

«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.»

(3) Quiconque contrevient aux dispositions du présent article 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 27. Exceptions au droit à l'information de la personne concernée

(1) L'article 26, paragraphes (1) et (2), ne s'applique pas lorsque le traitement est nécessaire pour sauvegarder :

(a) la sûreté de l'Etat ;

(b) la défense ;

(c) la sécurité publique ;

(Loi du 27 juillet 2007)

«(d) la prévention, la recherche, la constatation et la poursuite d'infractions pénales y compris celles à la lutte contre le blanchiment, ou le déroulement d'autres procédures judiciaires ;»

(e) un intérêt économique ou financier important de l'Etat ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal ;

(f) la protection de la personne concernée ou des droits et libertés d'autrui ;

(Loi du 27 juillet 2007)

«(g) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux lettres (c), (d) et (e).

(2) Les dispositions de l'article 26 sont susceptibles de dérogations lors de la collecte de données dans les cas prévus à l'article 9, lettres (c) et (d).»

(3) Les dispositions de l'article 26 paragraphes (1) et (2) ne s'appliquent pas lorsque, en particulier pour un traitement ayant une finalité statistique, historique ou

scientifique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si l'enregistrement ou la communication des données est prévu par la loi.

(4) Quiconque contrevient aux dispositions des paragraphes (1) et (2) qui précèdent 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions des paragraphes (1) et (2) du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 28. Droit d'accès

(1) Sur demande à introduire auprès du responsable du traitement, la personne concernée ou ses ayants droit justifiant d'un intérêt légitime peuvent obtenir sans frais, à des intervalles raisonnables et sans délais excessifs :

(a) l'accès aux données la concernant ;

(b) la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, sur les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées ;

(c) la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données ;

(d) la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 31.

(2) Celui qui entrave sciemment par quelque moyen que ce soit, l'exercice du droit d'accès, sera 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.

(3) Le patient a un droit d'accès aux données le concernant. Le droit d'accès est exercé par le patient lui-même ou par l'intermédiaire d'un médecin qu'il désigne. En cas de décès du patient, son conjoint non séparé de corps et ses enfants ainsi que toute personne qui au moment du décès a vécu avec lui dans le ménage ou, s'il s'agit d'un mineur, ses père et mère, peuvent exercer, par l'intermédiaire d'un médecin qu'ils désignent, le droit d'accès dont question à l'alinéa qui précède.

Le droit d'accès du patient pourra encore être exercé, du vivant d'une personne placée sous le régime de la curatelle ou sous celui de la tutelle tel qu'il est organisé par la loi du 11 août 1982, par l'intermédiaire d'un médecin désigné par son curateur ou tuteur.

(…) abrogé par la loi du 27 juillet 2007

(4) Selon le cas, le responsable du traitement procédera à la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente loi, notamment en raison du caractère incomplet ou inexact des données, sous peine d'encourir dans les conditions de l'article 33 l'interdiction temporaire ou définitive du traitement ou la destruction des données.

(5) Toute personne qui dans l'exercice de son droit d'accès a des raisons sérieuses d'admettre que les données qui lui ont été communiquées ne sont pas conformes aux données traitées, peut en informer la Commission nationale qui procède aux vérifications nécessaires.

(6) Toute rectification, tout effacement ou verrouillage effectué conformément au paragraphe (4) sera notifié sans délai par le responsable du traitement aux destinataires auxquels les données ont été communiquées, à moins que cela ne s'avère impossible.

(7) Sans préjudice de la sanction prévue au paragraphe (4), quiconque contrevient sciemment aux dispositions du présent article ou quiconque prend sciemment un nom ou prénom supposé ou une fausse qualité pour obtenir communication des données faisant l'objet d'un traitement en application du paragraphe (1), 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.

Art. 29. Exceptions au droit d'accès

(1) Le responsable du traitement peut limiter ou différer l'exercice du droit d'accès d'une personne concernée lorsqu'une telle mesure est nécessaire pour sauvegarder:

(a) la sûreté de l'Etat ;

(b) la défense ;

(c) la sécurité publique ;

(Loi du 27 juillet 2007)

«(d) la prévention, la recherche, la constatation et la poursuite d'infractions pénales, y compris celles à la lutte contre le blanchiment, ou le déroulement d'autres procédures judiciaires ;»

(e) un intérêt économique ou financier important de l'Etat ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal ;

(f) la protection de la personne concernée ou des droits et libertés d'autrui ;

(Loi du 27 juillet 2007)

«(g) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux lettres (c), (d) et (e).»

(…) abrogée par la loi du 27 juillet 2007

(2) Au cas où il n'existe manifestement aucun risque d'atteinte à la vie privée d'une personne concernée, le responsable du traitement peut limiter le droit d'accès lorsque les données sont traitées exclusivement aux fins de recherche scientifique ou sont stockées sous la forme de données pendant une durée n'excédant pas celle nécessaire à la seule finalité d'établissement de statistiques et que ces données ne puissent être utilisées aux fins de prendre une mesure ou une décision se rapportant à des personnes précises.

(Loi du 27 juillet 2007)

«(3) Dans le cadre d'un traitement de données à caractère personnel effectué à des fins de journalisme ou d'expression artistique ou littéraire, toute personne a un droit d'accès aux données la concernant.

Toutefois, dans tous les cas, le droit d'accès de la personne concernée aux données la concernant et utilisées dans le cadre d'un traitement mis en œuvre aux fins de journalisme ou d'expression artistique ou littéraire est limité dans la mesure où il ne peut pas porter sur des informations relatives à l'origine des données et qui permettraient d'identifier une source. Sous cette réserve l'accès doit être exercé par l'intermédiaire de la Commission nationale pour la protection des données en présence du Président du Conseil de Presse ou de son représentant, ou le Président du Conseil de Presse dûment appelé.»

(4) Le responsable du traitement doit indiquer le motif pour lequel il limite ou diffère l'exercice du droit d'accès.

Lorsque le droit d'accès est différé, le responsable du traitement doit indiquer la date à partir de laquelle le droit d'accès peut à nouveau être exercé. Le responsable du traitement notifiera le motif à la Commission nationale.

(5) 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.

(6) Quiconque contrevient à la disposition du paragraphe (4) qui précède 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.

Art. 30. Droit d'opposition de la personne concernée

(1) Toute personne concernée a le droit :

(a) de s'opposer à tout moment pour des raisons prépondérantes et légitimes tenant à sa

situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de dispositions légales prévoyant expressément le traitement.

En cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne peut pas porter sur ces données ;

(Loi du 27 juillet 2007)

(b) de s'opposer, sur demande et gratuitement, au traitement la concernant envisagé par le responsable du traitement «des données» à des fins de prospection ; il incombe au responsable du traitement de porter l'existence de ce droit à la connaissance de la personne concernée ;

(c) d'être informée avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

(2) Quiconque contrevient sciemment aux dispositions du présent article 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.

Art. 31. Décisions individuelles automatisées

Une personne peut être soumise à une décision individuelle automatisée produisant des effets juridiques à son égard, si cette décision :

(a) est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telle que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime, ou

(b) est autorisée par la loi, qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

Chapitre VII. Contrôle et surveillance de l'application de la loi

Art. 32. Missions et pouvoirs de la Commission nationale

(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.

(Loi du 27 juillet 2007)

(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 (5)», de la présente loi.

(6) Si la Commission nationale est saisie par l'une des personnes ou organes visés à l'article L. 261-1 paragraphe (2) du Code du Travail, 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.

(11) Quiconque empêche ou entrave sciemment, de quelque manière que ce soit, l'accomplissement des missions 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.

Art. 33. Sanctions administratives

(1) La Commission nationale peut prendre les sanctions disciplinaires suivantes :

(a) avertir ou admonester le responsable du traitement ayant violé les obligations lui imposées par les articles 21 à 24 ;

(b) verrouiller, effacer ou détruire des données faisant l'objet d'un traitement contraire aux dispositions de la présente loi ou de ses règlements d'exécution ;

(c) interdire temporairement ou définitivement un traitement contraire aux dispositions de la présente loi ou à ses règlements d'exécution ;

(d) ordonner l'insertion intégrale ou par extraits de la décision d'interdiction par la voie des journaux ou de toute autre manière, aux frais de la personne sanctionnée.

(2) Les décisions ci-dessus sont susceptibles d'un recours en réformation suivant l'article 3 de la loi du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif.

Art. 34. Composition de la Commission nationale

(1) La Commission nationale est une autorité publique qui prend la forme d'un établissement public. Son siège est fixé à Luxembourg-ville. Il peut être transféré à tout moment dans toute autre localité du Luxembourg par voie de règlement grand-ducal.

La Commission nationale dispose de la personnalité juridique et jouit de l'autonomie financière et administrative, sous la tutelle du ministre.

Elle exerce en toute indépendance les missions dont elle est investie en vertu de la présente loi.

(2) La Commission nationale est composée de trois membres effectifs et de trois membres suppléants nommés et révoqués par le Grand-Duc sur proposition du Gouvernement en conseil. Le président est désigné par le Grand-Duc. Les membres sont nommés pour un terme de six ans, renouvelable une fois.

Le Gouvernement en conseil propose au Grand-Duc comme membre effectif et suppléant chaque fois au moins un juriste et un informaticien justifiant d'une formation universitaire accomplie.

Avant d'entrer en fonction, le président de la Commission nationale prête entre les mains du Grand-Duc ou de son représentant le serment suivant : «Je jure fidélité au Grand-Duc, obéissance à la constitution et aux lois de l'Etat. Je promets de remplir mes fonctions avec intégrité, exactitude et impartialité.»

Avant d'entrer en fonction, les membres de la Commission nationale prêtent entre les mains du président de la Commission nationale le serment suivant : «Je jure fidélité au Grand-Duc, obéissance à la constitution et aux lois de l'Etat. Je promets de remplir mes fonctions avec intégrité, exactitude et impartialité.»

Lorsque le président ou un membre effectif de la Commission nationale est issu du secteur public, il obtient un congé spécial pour la durée de son mandat avec maintien de tous les avantages et droits découlant de son statut respectif. Il continue notamment à jouir de son traitement, indemnité ou salaire suivant le cas, ainsi que du régime de sécurité sociale correspondant à son statut.

(Loi du 27 juillet 2007)

«Par traitement, indemnité ou salaire au sens du présent article on entend l'émolument fixé pour les différentes fonctions physiques au moment de sa nomination, y compris toutes les majorations pour ancienneté de service, avancements et promotions auxquels le fonctionnaire, employé ou ouvrier peut prétendre en vertu d'une disposition légale, d'une disposition réglementaire prise en vertu d'une loi et du contrat collectif des ouvriers de l'Etat, s'il avait continué à faire partie de son administration ou établissement d'origine.

Ne sont pas compris dans le terme traitement, indemnité et salaire, les remises, droits casuels, indemnités de voyage ou de déplacement, frais de bureau et autres lorsqu'ils ne sont pas à considérer, d'après les dispositions qui les établissent, comme

constituant une partie intégrante du traitement, de l'indemnité ou du salaire.

(…)

En cas de cessation de mandat, le membre concerné est réintégré sur sa demande dans son administration d'origine à un emploi correspondant aux grade et échelon atteints à la fin de son mandat.»

A défaut de vacance, il peut être créé un emploi hors cadre correspondant à ce traitement ; cet emploi est supprimé de plein droit à la première vacance qui se produit dans une fonction appropriée du cadre normal.

Lorsque le président ou un membre effectif de la Commission nationale est issu du secteur privé, il touche une rémunération calculée par référence à la réglementation fixant le régime des indemnités des employés occupés dans les administrations et services de l'Etat qui est applicable en la matière, sur base d'une décision individuelle prise en vertu de l'article 23 du règlement grand-ducal du 28 juillet 2000 fixant le régime des indemnités des employés occupés dans les administrations et services de l'Etat. Il reste affilié au régime de sécurité sociale auquel il était soumis pendant l'exercice de sa dernière occupation.

En cas de cessation du mandat, il touche pendant une durée maximale d'un an une indemnité d'attente mensuelle correspondant au salaire ou traitement mensuel moyen du dernier revenu professionnel cotisable annuel mis en compte au titre de sa carrière d'assurance en cours avant le début de sa fonction de président ou de membre effectif de la Commission nationale. Cette indemnité d'attente est réduite dans la mesure où l'intéressé touche un revenu professionnel ou bénéficie d'une pension personnelle.

Le président et les membres effectifs de la Commission nationale bénéficient d'une indemnité spéciale tenant compte de l'engagement requis par les fonctions, à fixer par règlement grand-ducal.

La démission d'un membre de la Commission nationale intervient de plein droit par l'atteinte de la limite d'âge de 65 ans.

Les membres suppléants touchent une indemnité dont le montant est fixé par règlement grand-ducal.

(3) Les membres de la Commission nationale ne peuvent être membre du Gouvernement, de la Chambre des Députés, du Conseil d'Etat ou du Parlement Européen ni exercer d'activité professionnelle ou détenir directement ou indirectement des intérêts dans une entreprise ou tout autre organisme opérant dans le champ des traitements de données.

(4) Si, en cours de mandat un membre de la Commission nationale cesse d'exercer ses fonctions, le mandat de son successeur est limité à la période restant à courir.

Art. 35. Fonctionnement de la Commission nationale

(1) La Commission nationale est un organe collégial. Elle établit son règlement intérieur comprenant ses procédures et méthodes de travail dans le mois de son installation. Le règlement intérieur est publié au Mémorial.

(2) Sous réserve des dispositions de la présente loi, le règlement intérieur fixe :

(a) les règles de procédure applicables devant la Commission nationale,

(b) les conditions de fonctionnement de la Commission nationale,

(c) l'organisation des services de la Commission nationale.

(3) Les membres effectifs de la Commission nationale sont convoqués par le président. La convocation est de droit à la demande de deux membres effectifs. La convocation précise l'ordre du jour.

Les membres effectifs empêchés d'assister à une réunion sont tenus d'en avertir leur suppléant et de lui continuer la convocation.

(4) La Commission nationale ne peut valablement siéger ni délibérer qu'à condition de réunir trois membres.

(5) Les membres de la Commission nationale ne peuvent siéger, délibérer ou décider dans aucune affaire dans laquelle ils ont un intérêt direct ou indirect.

(6) Les délibérations sont prises à la majorité des voix. Les abstentions ne sont pas recevables.

(7) Le Gouvernement en conseil ayant proposé à la nomination un membre de la Commission nationale peut proposer sa révocation au Grand-Duc. La Commission nationale est entendue en son avis avant toute révocation.

(8) Dans l'exercice de leurs fonctions, les membres et les suppléants de la Commission nationale ne reçoivent d'instruction d'aucune autorité.

Art. 36. Statut des membres et agents de la Commission nationale

(Loi du 27 juillet 2007)

«(1) Le cadre du personnel de la Commission nationale comprend les fonctions et emplois suivants :

a) dans la carrière supérieure de l'attaché de direction, grade de computation de la bonification d'ancienneté : grade 12,

- des conseillers de direction 1re classe ;
- des conseillers de direction ;
- des conseillers de direction adjoints ;
- des attachés de direction 1ers en rang ;
- des attachés de direction.

b) dans la carrière supérieure de l'ingénieur, grade de computation d'ancienneté : grade 12,

- des ingénieurs 1re classe ;
- des ingénieurs-chef de division ;
- des ingénieurs principaux ;
- des ingénieurs-inspecteurs ;
- des ingénieurs.

c) dans la carrière moyenne de l'ingénieur technicien, grade de computation de la bonification d'ancienneté : grade 7,

- des ingénieurs techniciens inspecteurs principaux 1ers en rang ;
- des ingénieurs techniciens inspecteurs principaux ;
- des ingénieurs techniciens-inspecteurs ;
- des ingénieurs techniciens principaux ;
- des ingénieurs techniciens.

d) dans la carrière moyenne du rédacteur, grade de computation de la bonification d'ancienneté : grade 7,

- des inspecteurs principaux 1ers en rang ;
- des inspecteurs principaux ;
- des inspecteurs ;
- des chefs de bureau ;
- des chefs de bureau adjoints ;
- des rédacteurs principaux ;
- des rédacteurs.

Les agents des carrières prévues ci-dessus sont des fonctionnaires de l'Etat.»

(2) Le cadre prévu au paragraphe (1) ci-dessus peut être complété par des employés de l'Etat ainsi que par des ouvriers de l'Etat dans les limites des crédits disponibles.

La rémunération des employés de l'Etat est fixée conformément au règlement grand-ducal du 28 juillet 2000 fixant le régime des indemnités des employés occupés dans les administrations et services de l'Etat.

(3) Les rémunérations et autres indemnités de tous membres, agents et employés de la Commission nationale sont à charge de la Commission nationale.

(4) La Commission nationale peut, dans des cas déterminés, faire appel à des experts externes dont les prestations sont définies et rémunérées sur la base d'un contrat de droit privé.

Art. 37. Dispositions financières

(1) Au moment de sa création, la Commission nationale bénéficie d'une dotation initiale de deux cent mille euros à charge du budget de l'Etat. L'Etat met à sa disposition les biens mobiliers et immobiliers

nécessaires au bon fonctionnement et à l'exercice de ses missions.

(2) L'exercice financier de la Commission nationale coïncide avec l'année civile.

(3) Avant le 31 mars de chaque année, la Commission nationale arrête son compte d'exploitation de l'exercice précédent, ensemble avec son rapport de gestion. Avant le 30 septembre de chaque exercice, la Commission nationale arrête le budget pour l'exercice à venir. Le budget, les comptes annuels et les rapports arrêtés sont transmis au Gouvernement en conseil qui décide de la décharge à donner à la Commission nationale. La décision constatant la décharge accordée à la Commission nationale ainsi que les comptes annuels de la Commission nationale sont publiés au Mémorial.

(Loi du 27 juillet 2007)

(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».

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.

(5) *abrogé par la loi du 27 juillet 2007*

Chapitre VIII. Recours juridictionnels

Art. 38. Généralités

Sans préjudice des sanctions pénales instituées par la présente loi et des actions en responsabilité régies par le droit commun, en cas de mise en œuvre d'un traitement en violation des formalités prévues par la présente loi toute personne dispose d'un recours juridictionnel tel que prévu ci-après :

Art. 39. Action en cessation

(1) A la requête

- du Procureur d'Etat qui a déclenché une action publique pour violation de la présente loi,
- de la Commission nationale, dans l'hypothèse où une sanction disciplinaire visée à l'article 33 de la présente loi, qui n'a pas fait l'objet d'un recours ou qui a été confirmée par la juridiction administrative, n'a pas été respectée, ou
- d'une personne lésée, dans l'hypothèse où la Commission nationale n'a pas pris position sur une saisine intervenue sur la base de l'article 32, paragraphe (4), (5) ou (6) de la présente loi, le président du tribunal d'arrondissement du lieu où le traitement est mis en œuvre, ou le juge qui le remplace, ordonne la cessation du traitement contraire aux dispositions de la présente loi et la suspension provisoire de l'activité du responsable du traitement ou du sous-traitant. Le président du tribunal d'arrondissement, ou le juge qui le remplace, peut ordonner la fermeture provisoire de l'établissement du responsable du traitement ou du sous-traitant lorsque sa seule activité est de traiter des données.

(2) L'action est recevable même lorsque le traitement illégal a pris fin ou n'est plus susceptible de se reproduire.

(3) L'action est introduite et jugée comme en matière de référé conformément aux articles 932 à 940 du Nouveau code de procédure civile. Toutefois, par dérogation à l'article 939, alinéa 2, du Nouveau code de procédure civile, l'ordonnance de référé n'est pas susceptible d'opposition.

(4) Sont également applicables les articles 2059 à 2066 du Code civil.

(5) La publication de la décision peut être ordonnée, en totalité ou par extrait, aux frais du contrevenant, par la voie des journaux ou de toute autre manière. Il ne peut être procédé à la publication qu'en vertu d'une décision judiciaire coulée en force de chose jugée.

(6) La suspension provisoire et le cas échéant la fermeture provisoire peuvent être ordonnées indépendamment de l'action publique. La suspension provisoire ou la fermeture provisoire ordonnée par le président du tribunal d'arrondissement, ou par le juge qui le remplace, prend toutefois fin en cas de décision de non-lieu ou d'acquittement, et au plus

tard à l'expiration d'un délai de deux ans à partir de la décision initiale de suspension ou de fermeture.

Chapitre IX. Le chargé de la protection des données

Art. 40. Le chargé de la protection des données

(Loi du 27 juillet 2007)

(1) Tout responsable de traitement peut (…) désigner un chargé de la protection des données, dont il communique l'identité à la Commission nationale.

(2) Les pouvoirs du chargé de la protection des données sont les suivants :

(a) un pouvoir d'investigation aux fins d'assurer la surveillance du respect des dispositions de la présente loi et de ses règlements d'exécution par le responsable du traitement ;

(b) un droit d'information auprès du responsable du traitement et corrélativement, un droit d'informer le responsable du traitement des formalités à accomplir afin de se conformer aux dispositions de la présente loi et de ses règlements d'exécution.

(Loi du 27 juillet 2007)

«(3) Dans l'exercice de ses missions le chargé de la protection des données est indépendant vis-à-vis du responsable du traitement qui le désigne.

Afin de pouvoir s'acquitter de ses missions, le chargé de la protection des données doit disposer d'un temps approprié.

Les missions ou activités exercées concurremment par le chargé de la protection des données ne doivent pas être susceptibles de provoquer un conflit d'intérêt avec l'exercice de sa mission.

(4) Le chargé de la protection des données ne peut faire l'objet de représailles de la part de l'employeur du fait de l'exercice de ses missions, sauf violation de ses obligations légales ou conventionnelles.»

(5) Le chargé de la protection des données consulte la Commission nationale en cas de doute quant à la conformité à la présente loi d'un traitement mis en œuvre sous sa surveillance.

(6) Peuvent être désignés à la fonction de chargé de la protection des données les personnes physiques et morales qui sont agréées par la Commission nationale.

(Loi du 27 juillet 2007)

(7) L'agrément pour l'activité du chargé de la protection des données est subordonné à la justification d'une formation universitaire accomplie en droit, économie, gestion d'entreprise, sciences de la nature, ou informatique (…).

(8) Par dérogation au paragraphe précédent, les membres inscrits dans une des professions réglementées suivantes peuvent être agréés comme chargé de la protection des données sans autre condition : avocat à la Cour, réviseur d'entreprises, expert-comptable, médecin.

Un règlement grand-ducal peut ajouter à cette liste d'autres professions réglementées et assujetties à un organisme de surveillance ou de discipline, soit officiel soit propre à la profession et reconnu par la loi.

(9) 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 :

(a) ne présente pas les qualités requises pour la fonction de chargé de la protection des données ; ou

(b) est d'ores et déjà en relation avec le responsable du traitement dans le cadre d'autres activités que celle du traitement des données et que cette relation fait naître un conflit d'intérêts limitant son indépendance.

En cas d'opposition de la Commission nationale, le responsable du traitement dispose de trois jours pour désigner un nouveau chargé de la protection des données.

(10) La Commission nationale définit les modalités du contrôle continu des qualités requises à la fonction de chargé de la protection des données.

(11) Un règlement grand-ducal fixera les modalités de désignation et de révocation du chargé de protection des données, d'exécution de ses missions, de même que ses relations avec la Commission nationale.

Chapitre X. Dispositions spécifiques, transitoires et finales

Art. 41. Dispositions spécifiques

(1) (a) Les autorités compétentes visées aux articles 88-1 à 88-4 du Code d'instruction criminelle, et

(b) les autorités agissant dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du Code d'instruction criminelle, accèdent de plein droit, sur requête et par l'intermédiaire de l'Institut luxembourgeois de régulation (ciaprès «ILR») aux données concernant l'identité des abonnés et utilisateurs des opérateurs et fournisseurs de communications électroniques ainsi que des services postaux et des fournisseurs de ces services.

(Loi du 27 juillet 2007)

«La centrale des secours d'urgence 112, les centres d'appels d'urgence de la police grand-ducale et la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg accèdent dans les mêmes conditions et modalités que les autorités visées à l'alinéa précédent aux seules données concernant l'identité des abonnés et utilisateurs des opérateurs et fournisseurs de communications électroniques.»

(2) A ces fins, les opérateurs et les fournisseurs mettent d'office et gratuitement à la disposition de l'ILR les données prescrites au paragraphe (1). Les données doivent être actualisées au moins une fois par jour.

L'accès doit être garanti vingt-quatre heures sur vingt-quatre et sept jours sur sept. Un règlement grand-ducal détermine les services de communications électroniques et services postaux pour lesquels les opérateurs et fournisseurs de services doivent mettre à disposition les données ainsi que la nature, le format et les modalités de mise à disposition des données.

(Loi du 27 juillet 2007)

«(3) L'accès de plein droit se limite aux mesures spéciales de surveillance telles que prévues aux articles 88-1 à 88-4 du Code d'instruction criminelle, celles prises en matière de crime flagrant ou dans le cadre de l'article 40 du Code d'Instruction criminelle et aux mesures particulières de secours d'urgence prestées dans le cadre des activités de la centrale des secours d'urgence 112, des centres d'appels d'urgence de la police grand-ducale et de la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg.»

(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.

(Loi du 27 juillet 2007)

«(5) L'autorité de contrôle visée à l'article 17, paragraphe (2) veille au respect du présent article.»

Art. 42. Dispositions transitoires

(1) Les traitements existant dans des fichiers non automatisés ou automatisés antérieurs à l'entrée en vigueur de la présente loi doivent être rendus conformes aux dispositions du chapitre II et du chapitre VI, dans un délai de deux ans à compter de la date d'entrée en vigueur de la présente loi.

(2) Toutefois la personne concernée peut obtenir, sur demande, et notamment en ce qui concerne l'exercice de son droit d'accès, la rectification, l'effacement ou le verrouillage des données incomplètes, inexactes ou conservées de manière incompatible aux fins légitimes poursuivies par le responsable du traitement.

(3) La Commission nationale peut permettre que les données conservées uniquement à des fins de recherche historiques soient dispensées de respecter le paragraphe (1).

(Loi du 27 juillet 2007)

«(4) Pour l'application des dispositions de l'article 34 ci-dessus, la rémunération de l'agent nommé le

14 octobre 2002 membre effectif de la Commission nationale pour la protection des données et titulaire d'un diplôme universitaire en informatique est fixée en supposant qu'une nomination fictive à la fonction d'attaché de gouvernement soit intervenue le 1er novembre 2002, qu'il ait bénéficié d'une promotion à la fonction d'attaché de gouvernement premier en rang le 1er novembre 2005 et qu'il bénéficierait d'une promotion à la fonction de conseiller de direction adjoint au plus tôt le 1er novembre 2008.»

Art. 43. Mise en vigueur des dispositions transitoires

(1) La Commission nationale établira le schéma de notification prévu à l'article 13, paragraphe (3), dans les quatre mois de la nomination de ses membres. Elle informera le public, moyennant publication au Mémorial et communiqué de presse aux journaux édités au Luxembourg, de la date à partir de laquelle le schéma de notification est disponible auprès de la Commission nationale.

(2) Les responsables du traitement procéderont à la notification de leurs traitements dans les quatre mois à partir de la date de la publication officielle mentionnée au paragraphe (1).

(3) Les responsables du traitement dont les traitements sont autorisés, lors de l'entrée en vigueur de la présente loi, moyennant règlement grand-ducal ou arrêté ministériel «autorisant la création et l'exploitation d'une banque de données», ne notifieront ou ne demanderont l'autorisation de leurs traitements qu'à l'expiration de la durée de validité de l'autorisation octroyée, à moins que pour des raisons de conformité avec les dispositions de la présente loi, ils jugent nécessaire de le faire auparavant.

(4) Les traitements non automatisés de données contenues ou appelées à figurer dans un fichier sont à notifier dans les douze mois à partir de la date de la publication officielle mentionnée au paragraphe (1).

Art. 44. Dispositions finales

(1) La loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques est abrogée.

(2) 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 vigueur tant qu'ils n'auront pas été remplacés par de nouvelles dispositions.

(Loi du 27 juillet 2007)

«(3) L'article 4 paragraphe (3) lettre d) de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques doit être modifié comme suit :

- à l'alinéa 1er, il y a lieu de compléter le bout de phrase «afin de fournir une preuve d'une transaction commerciale» par «afin de fournir une preuve d'une transaction commerciale ou de toute autre communication commerciale» ;

- à l'alinéa 2, la première phrase débute comme suit : «Les parties aux transactions ou à toutes autres communications commerciales….»

(4) Aux articles 5 paragraphe (1) lettre a) et 9 paragraphe (1) lettre a) de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques la durée de «12 mois» est remplacée par celle de «6 mois».

(5) L'article 12 de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques est complété à la fin par l'ajout suivant «(…) sans préjudice de l'application de l'article 8 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel».

(6) L'article 23 de la loi du 8 juin 2004 sur la liberté d'expression dans les médias est modifié comme suit :

Au point 1. du paragraphe (2) est rajouté après les mots «et éditeurs» le bout de phrase suivant : «y compris dans le domaine des traitements de données à caractère personnel».

Au point 2 du même paragraphe est intercalé entre les mots «par la voie d'un média» et «sans préjudice des pouvoirs réservés» le bout de phrase suivant : «y compris des plaintes concernant le respect des droits

et libertés des personnes en matière de traitement des données à caractère personnel.»»

Art. 45. Entrée en vigueur

La présente loi entre en vigueur le premier jour du quatrième mois qui suit sa publication au Mémorial.

Par dérogation à ce qui précède, les articles 34, 35, 36 et 37 entrent en vigueur trois jours après publication de la présente loi au Mémorial.