CHAMBRE DES DÉPUTÉS
GRAND-DUCHÉ DE LUXEMBOURG

Dossier consolidé

Projet de loi 4735

Projet de loi relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

Date de dépôt : 07-12-2000
Date de l'avis du Conseil d'État : 29-01-2002

Liste des documents

Date	Description	Nom du document	Page
07-12-2000	Déposé	4735/00	3
22-05-2001	Avis de la Chambre des Fonctionnaires et Employés publics (22.5.2001)	4735/01	112
05-07-2001	Avis du Procureur d'Etat (5.7.2001)	4735/02	121
30-10-2001	Avis de la Chambre des Employés Privés (30.10.2001)	4735/04	130
14-11-2001	Avis de la Chambre de Travail (14.11.2001)	4735/03	139
22-11-2001	Avis de la Chambre des Métiers (22.11.2001)	4735/05	151
14-01-2002	A la demande de Monsieur le Ministre délégué aux Communications en date du 14.1.2002, le document parlementaire N°4735/2 concernant le projet de loi repris sous rubrique est retiré et est à considérer [...]	4735/02A	164
29-01-2002	Avis du Conseil d'Etat (29.1.2002)	4735/06	167
13-02-2002	Avis de la Chambre de Commerce (13.2.2002) - Dépêche du Ministre aux Relations avec le Parlement au Président de la Chambre des Députés (19.6.2002)	4735/09	204
15-05-2002	Rapport pour avis de la Commission du Travail et de l'Emploi (15.5.2002)	4735/07	217
06-06-2002	Amendements adoptés par la/les commission(s) : Commission des Media et des Communications	4735/08	224
02-07-2002	Avis complémentaire du Conseil d'Etat (2.7.2002)	4735/10	265
04-07-2002	Amendements adoptés par la/les commission(s) : Commission des Media et des Communications	4735/11	277
09-07-2002	Deuxième avis complémentaire du Conseil d'Etat (9.7.2002)	4735/12	304
10-07-2002	Rapport de commission(s) : Commission des Media et des Communications Rapporteur(s) :	4735/13	307
19-07-2002	Dispense du second vote constitutionnel par le Conseil d'Etat (19-07-2002) Evacué par dispense du second vote (19-07-2002)	4735/14	379
17-07-2002	Traitement de données à caractère personnel	Document écrit de dépot	382
31-12-2002	Publié au Mémorial A n°91 en page 1836	4735	384

4735/00

N° 4735

CHAMBRE DES DEPUTES

Session ordinaire 2000-2001

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

(Dépôt: le 7.12.2000)

SOMMAIRE:

		page
1)	Arrêté Grand-Ducal de dépôt (7.12.2000)	1
2)	Texte du projet de loi	2
3)	Commentaire des articles	24
4)	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	53
5)	Exposé des motifs	77

*

ARRETE GRAND-DUCAL DE DEPOT

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Sur le rapport de Notre Ministre délégué aux Communications et après délibération du Gouvernement en Conseil;

Arrêtons:

Article unique.– Notre Ministre délégué aux Communications présentera en Notre Nom à la Chambre des Députés le projet de loi relatif à la protection des personnes à l'égard du traitement des données à caractère personnel.

Palais de Luxembourg, le 7 décembre 2000

Le Ministre délégué aux Communications,
François BILTGEN

HENRI

*

TEXTE DU PROJET DE LOI

Chapitre I. *Dispositions générales*

Art. 1er. *Objet*

La présente loi protège la vie privée ainsi que les libertés et les droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel et fait respecter les intérêts légalement protégés des personnes morales.

Art. 2. *Définitions*

Aux fins de la présente loi, on entend par:

(a) „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 ou morale est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique;

(b) „personne concernée": toute personne physique ou morale, publique ou privée ou groupement de fait sujet d'un traitement de données à caractère personnel;

(c) „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;

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

(e) „interconnexion": toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour une autre finalité par le même responsable du traitement ou par un ou d'autres responsables du traitement;

(f) „ministre": le ministre ayant dans ses attributions la protection des données;

(g) „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;

(h) „surveillance": toute activité faisant appel à des moyens techniques en vue de détecter, d'observer et/ou de copier et/ou d'enregistrer intentionnellement les mouvements et/ou les paroles et/ou les écrits et/ou l'état d'un objet ou d'une personne fixe ou mobile;

(i) „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;

(j) „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;

(k) „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 d'une mission d'enquête particulière ne sont pas considérées comme des destinataires;

(l) „consentement de la personne concernée“: toute manifestation de volonté non équivoque, 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;

(m) „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 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;

(o) „pays tiers“: Etat non membre de l'Union européenne;

(p) „la Commission“: la Commission nationale pour la protection des données.

(q) „instance médicale“: toute personne physique ou morale autorisée à exercer soit des activités ayant pour objet la prévention, le diagnostic ou le traitement de maladies et infirmités, soit des activités de soins, soumise au secret professionnel au sens de l'article 458 du code pénal;

(r) „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, ainsi que des prestations familiales ou d'aides sociales.

Art. 3. ***Champ d'application***

(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.

(2) La présente loi s'applique au traitement lorsqu'il est mis en oeuvre:

(a) par un responsable du traitement établi sur le territoire luxembourgeois ou en un lieu où, selon le droit international public, est applicable le droit luxembourgeois;

(b) par un responsable du traitement qui n'est pas établi sur le territoire d'un des Etats membres de l'Union européenne et qui recourt à des fins de traitement à des moyens, automatisés ou non, situés sur le territoire luxembourgeois, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire luxembourgeois; dans ce cas, le responsable du traitement désigne, par une déclaration écrite à la Commission, un représentant établi sur le territoire luxembourgeois qui se substitue aux droits et obligations du responsable du traitement sans que ce dernier ne soit dégagé de son éventuelle responsabilité particulière.

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

(4) La présente loi s'applique à toute forme de captage, de traitement et de diffusion de sons et images qui permettent d'identifier des personnes physiques ou morales.

(5) La présente loi s'applique au traitement ayant pour objet la sécurité publique, la défense, les activités relatives à des domaines du droit pénal, la sûreté de l'Etat ou le bien-être économique de l'Etat lorsque celui-ci est lié à la sûreté de l'Etat, sans préjudice des dispositions spécifiques contenues dans les instruments de droit international qui lient le Grand-Duché de Luxembourg et des dispositions légales spécifiques dans ces domaines respectifs.

Chapitre II. *Conditions de licéité du traitement*

Art. 4. ***Qualité des données***

(1) Le responsable du traitement doit garantir 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.

(2) Les données traitées à des finalités déterminées peuvent être traitées ultérieurement à des fins historiques, statistiques ou scientifiques dans les conditions prévues par le régime d'autorisation préalable de la Commission visé à l'article 14.

(3) Quiconque effectue un traitement en violation des dispositions de cet article est puni d'un emprisonnement de huit jours à six mois et d'une amende de 10.001 à 3.000.000 LUF, ou d'une de ces peines seulement.

Art. 5. ***Légitimité du traitement***

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

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

(b) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, ou si

(c) le traitement 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 si

(d) le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, ou si

(e) le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou si

(f) la personne concernée a donné son consentement exprès.

(2) Quiconque effectue un traitement en violation des dispositions de cet article est puni d'un emprisonnement de huit jours à six mois et d'une amende de 10.001 à 3.000.000 LUF, ou d'une de ces peines seulement.

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.

Aux fins de la présente loi, on entend par:

(a) „donnée relative à la santé“: toute information concernant l'état physique et mental d'une personne concernée, y compris certaines données génétiques, de même que les informations sociales et administratives connexes susceptibles d'avoir une incidence sur cet état;

(b) „donnée génétique“: toute donnée, quel qu'en soit le type, qui concerne les caractères héréditaires d'un individu ou qui est en rapport avec de tels caractères formant le patrimoine d'un groupe d'individus apparentés.

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

(a) la personne concernée a donné son consentement exprès à un tel traitement, sauf indisponibilité du corps humain et sauf le cas où la loi prévoit que l'interdiction visée au paragraphe (1) ne peut être levée par le consentement de la personne concernée, ou lorsque

(b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement notamment en matière de droit du travail dans la mesure où il est autorisé par disposition légale, 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 oeuvre, 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 exprès des personnes concernées, ou lorsque

(e) le traitement porte sur des données manifestement rendues publiques par la personne concernée ou dès lors que son consentement au traitement des données peut légitimement être déduit de ses déclarations, ou lorsque

(f) le traitement mis en oeuvre conformément aux règles de procédures judiciaires applicables est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice s'il est mis en oeuvre à cette fin exclusive, ou lorsque

(g) le traitement s'avère nécessaire pour un motif d'intérêt public important notamment à des fins historiques, statistiques ou scientifiques et que ce traitement est mis en oeuvre conformément au régime d'autorisation préalable de la Commission tel que prévu à l'article 14, ou lorsque

(h) le traitement est mis en oeuvre par voie de règlement grand-ducal tel que prévu à l'article 17.

(3) L'article 6 paragraphe (1) ne s'applique pas lors d'une procédure judiciaire ou d'une enquête pénale. Toutefois les données génétiques ne peuvent être traitées que pour vérifier l'existence d'un lien génétique dans le cadre de l'administration de la preuve en justice, pour la prévention d'un danger concret ou pour la répression d'une infraction pénale déterminée.

(4) Les données génétiques peuvent être traitées :

(a) dans les cas visés par les articles 6 paragraphe (2) (c), (f), (g), (h), 6 paragraphe (3) et 7 de la présente loi, ou

(b) lorsque la personne concernée a donné son consentement exprès et si le traitement est effectué dans les seuls domaines de la santé ou de la recherche scientifique sauf indisponibilité du corps humain et 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.

(5) 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 10.001 à 5.000.000 LUF, ou d'une de ces peines seulement.

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

(1) Lorsque le traitement de données tel que défini à l'article 6 paragraphe (1) de la présente loi est 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, de la recherche scientifique dans le domaine de la biologie et de la médecine; le traitement de ces données peut être mis en oeuvre par des instances médicales, ainsi que par les organismes de sécurité sociale et les administrations qui gèrent ces données en exécution de leurs missions légales et réglementaires et lorsque le responsable du traitement est soumis au secret professionnel. Le recours à un sous-traitant est possible dans les conditions de confidentialité prévues à l'article 21.

(2) Le traitement visé à l'article 7 paragraphe (1) fait l'objet d'une autorisation préalable de la Commission.

(3) Par dérogation au paragraphe (2) qui précède est soumis à notification:

– le traitement mis en oeuvre conformément à l'article 36 de la loi du 28 août 1998 sur les établissements hospitaliers;
– le traitement mis en oeuvre par un médecin et concernant ses patients.

(4) En application des articles 6 et 7 un règlement grand-ducal établit:

(a) les modalités et les conditions d'après lesquelles les données visées à l'article 6 paragraphe (1) de la loi peuvent être communiquées à un tiers;
(b) les modalités et les conditions d'après lesquelles les données visées à l'article 6 paragraphe (1) de la loi peuvent être utilisées à des fins de recherche;

(5) Quiconque effectue un traitement en violation des dispositions de cet article est puni d'un emprisonnement de huit jours à un an et d'une amende de 10.001 à 5.000.000 LUF, ou d'une de ces peines seulement.

Art. 8. ***Traitement de données judiciaires***

(1) Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être mis en oeuvre qu'en exécution d'une disposition légale.

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

(3) Les données relatives aux jugements civils ou administratifs, de même que les sanctions administratives sont traitées sous le contrôle de l'autorité publique compétente en la matière.

(4) Quiconque effectue un traitement en violation des dispositions de cet article est puni d'un emprisonnement de huit jours à un an et d'une amende de 10.001 à 5.000.000 LUF, ou d'une de ces peines seulement.

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

(1) Dans la mesure où il s'avère nécessaire pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression, le traitement mis en oeuvre aux seules fins de journalisme ou d'expression artistique ou littéraire n'est pas soumis:

(a) lorsque le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou à des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée;
    – 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
(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 paragraphes (1) et (2), lorsque leur application compromettrait la collecte des données auprès de la personne concernée et
    – de l'article 26 paragraphe (3), 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,
(d) au droit d'accès de la personne concernée qui peut être différé ou limité conformément à l'article 28 paragraphe (4) et à l'article 29.

(2) Lors de la notification d'un traitement effectué à des fins de journalisme ou d'expression artistique ou littéraire, la notification ne renseigne que sur le(s) nom(s) et adresse(s) du responsable du traitement ou de son représentant.

(3) La Commission, conformément aux pouvoirs qui lui sont conférés par la présente loi et dans le respect des règles relatives à la liberté d'expression, ne peut opérer qu'en présence du président de l'organe représentatif de la presse ou de son délégué, dès lors qu'un traitement visé au paragraphe (1) est impliqué.

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 exprès, ou

(b) aux abords ou dans tout lieu accessible ou non au public, notamment dans les parkings couverts, les gares et aérogares et les moyens de transports publics, pourvu qu'il présente dans sa situation, sa configuration ou sa fréquentation un risque rendant traitement nécessaire à la prévention, la recherche, la constatation et la poursuite infractions pénales, ou

(c) dans une résidence privée dont le responsable du traitement est la personne physique y domiciliée.

(2) Sans préjudice du droit à l'information prévu à l'article 26, 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 oeuvre des traitements visés au paragraphe (1).

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

(a) si la personne concernée a donné son consentement exprès nonobstant des dispositions contraires de la loi, ou

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

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

(4) Le traitement à des fins de surveillance exclusivement mis en oeuvre pour la prévention des infractions pénales est soumis à l'obligation d'information excluant ainsi application de l'article 27 paragraphe (1) (d).

(5) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 10.001 à 5.000.000 LUF ou d'une des peines seulement.

Art. 11. ***Traitement à des fins de surveillance sur le lieu de travail***

(1) Le traitement à des fins de surveillance sur le lieu de travail peut être mis en oeuvre, conformément à l'article 14, par l'employeur s'il en est le responsable. Un tel traitement n'est possible que s'il est nécessaire:

(a) pour les besoins de sécurité et de santé des travailleurs, ou

(b) pour les besoins de protection des biens de l'entreprise, ou

(c) pour le contrôle du processus de production portant uniquement sur les machines, ou

(d) pour le contrôle temporaire de production ou des prestations du travailleur en vue de mesurer son activité afin de déterminer sa rémunération.

Dans les cas visés aux lettres (a) et (d), le comité mixte d'entreprise, le cas échéant institué, a un pouvoir de décision tel que défini à l'article 7 paragraphes (1) et (2) de la loi du 6 mai 1974 instituant des comités mixtes dans les entreprises du secteur privé et organisant la représentation des salariés dans les sociétés anonymes.

Le consentement exprès de la personne concernée ne rend pas légitime le traitement mis en oeuvre par l'employeur .

(2) Sans préjudice du droit à l'information de la personne concernée celle-ci ainsi que le comité mixte ou à défaut la délégation du personnel ou à défaut encore l'Inspection du Travail et des Mines sont informés par l'employeur:

(a) de la finalité du traitement auquel les données sont destinées,

(b) de la ou des périodes pendant lesquelles la surveillance sera effectuée,

(c) de la durée et le cas échéant des conditions de conservation des données.

(3) Quiconque contrevient aux dispositions du présent article est puni d'une peine d'emprisonnement de huit jours à un an et d'une amende de 10.001 à 5.000.000 LUF, ou d'une des peines seulement.

Chapitre III. *Notification et publicité des traitements*

Art. 12. *Obligation de notification à la Commission*

(1) Préalablement à la mise en oeuvre d'un traitement ou d'un ensemble de traitements ayant une même finalité ou des finalités liées, le responsable du traitement, ou son représentant, la notifie à la Commission.

(2) Est exempté de l'obligation de notification:

(a) le responsable du traitement qui désigne un chargé de la protection des données tenu notamment d'assurer, de manière indépendante, l'application des dispositions légales en la matière et d'établir un registre des traitements effectués par le responsable du traitement conformément aux dispositions relatives à la publicité des traitements telles que prévues à l'article 15;

(b) le traitement ayant pour seul objet 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) le traitement soumis à l'autorisation par voie réglementaire prévue à l'article 17;

(d) le traitement mis en oeuvre conformément aux règles de procédures judiciaires et nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice.

(3) Quiconque ne se soumet pas à l'obligation de notification telle que prévue au paragraphe (1) qui précède est puni d'une amende de 10.001 à 1.000.000 LUF.

(4) Quiconque fournit lors de la notification sciemment des informations incomplètes ou inexactes est puni d'un emprisonnement de huit jours à six mois et d'une amende de 10.001 à 3.000.000 LUF, ou d'une de ces peines seulement.

Art. 13. *Contenu et forme de la notification*

(1) La notification comprend au moins les informations suivantes:

(a) le nom et l'adresse du responsable du traitement ou de son représentant et le cas échéant du sous-traitant;

(b) la ou les finalités du traitement;

(c) la description de la ou des catégories de personnes concernées et des données ou des catégories de données s'y rapportant;

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

(e) les pays tiers à destination desquels des transferts de données sont envisagés;

(f) 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;

(g) la durée de conservation des données.

(2) Toute modification affectant les informations visées au paragraphe (1) doit être notifiée à la Commission préalablement à la mise en oeuvre du traitement.

(3) La notification se fait auprès de la Commission moyennant support papier ou informatique suivant un schéma à établir par elle. Il est accusé réception de la notification.

(4) Quiconque contrevient aux dispositions des paragraphes (1) et (2) qui précèdent est puni d'une amende de 10.001 à 1.000.000 LUF.

(5) Un règlement grand-ducal fixera le montant et les modalités de paiement d'une redevance à percevoir lors de toute notification et de toute modification de notification.

Art. 14. ***Autorisation préalable de la Commission***

(1) Sont soumis à l'autorisation préalable de la Commission:

(a) les traitements prévus aux articles 6 paragraphe (2) a), b), e), g), 6 paragraphe (4) b), 11 et le cas échéant ceux prévus à l'article 7 de la présente loi;

(b) les traitements de données à des fins historiques, statistiques ou scientifiques visés à l'article 4 paragraphe (2). La Commission vérifie en particulier si ces traitements ne peuvent être réalisés sur base de données rendues anonymes;

(c) l'interconnexion de données à caractère personnel visée à l'article 16;

(d) le traitement concernant le crédit et la solvabilité des personnes concernées;

(e) l'utilisation de données à caractère personnel à des fins autres que celles pour lesquelles elles ont été collectées.

(2) L'autorisation n'est délivrée par la Commission qu'après examen préalable à la mise en oeuvre des traitements visés au paragraphe (1). L'examen préalable est effectué dès la réception de la notification. L'autorisation à délivrer en matière de traitement à des fins de surveillance sur le lieu de travail est subordonnée à l'avis préalable de l'Inspection du Travail et des Mines.

(3) Quiconque effectue un traitement en violation des dispositions de cet article est puni d'un emprisonnement de huit jours à un an et d'une amende de 10.001 à 5.000.000 LUF, ou d'une de ces peines seulement.

Art. 15. ***Publicité des traitements***

(1) La Commission tient un registre des traitements qui lui sont notifiés en vertu de l'article 12, paragraphe (1). Ce registre contient sur chaque traitement les informations énumérées à l'article 13, paragraphe (1) de la présente loi.

(2) Pour les traitements soumis à l'autorisation préalable, le registre renseigne en plus sur l'autorisation émise par la Commission.

(3) Toute personne peut prendre connaissance gratuitement des informations contenues dans le registre à l'exception de celles prévues à l'article 13 paragraphe (1) (f).

(4) La Commission publie un rapport annuel qui fait état des notifications et autorisations.

(5) 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 à caractère personnel***

(1) L'interconnexion de données à caractère personnel qui n'est pas expressément prévue par un texte légal doit faire l'objet d'une autorisation préalable de la Commission demandée par les responsables des traitements conjointement.

(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.

(3) Un règlement grand-ducal peut déterminer les modalités de mise en oeuvre des traitements visés au paragraphe (1).

Art. 17. ***Autorisation par voie réglementaire***

Font l'objet d'un règlement grand-ducal:

(1) les traitements d'ordre général nécessaires à la prévention, à la recherche, à la constatation et à la poursuite des infractions pénales qui sont réservés, conformément à leurs missions légales et réglemen-

taires respectives, aux organes du corps de la police grand-ducale, de l'Inspection générale de police et de l'administration des douanes et accises. Leur responsable est le Procureur d'Etat territorialement compétent. Le règlement grand-ducal déterminera notamment le Procureur d'Etat 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,

(2) les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique.

(3) Quiconque effectue un traitement en violation des dispositions de cet article est puni d'un emprisonnement de huit jours à un an et d'une amende de 10.001 à 5.000.000 LUF, ou d'une de ces peines seulement.

Chapitre IV. *Transferts de données vers des pays tiers*

Art. 18. *Principes*

(1) Le transfert de données faisant l'objet d'un traitement après leur transfert vers un Etat non membre de l'Union européenne, 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 pour la protection des données qui apprécie si un pays tiers assure un niveau de protection adéquat. La Commission nationale pour la protection des données 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 pour la Protection des Données 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 10.001 à 5.000.000 LUF, ou d'une de ces peines seulement.

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 exprès 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 la vie de la personne concernée, ou

(f) le transfert intervienne depuis un registre public tel que prévu à l'article 12 paragraphe (2) (b).

(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 notifier à la Commission un rapport établissant les conditions dans lesquelles il a opéré le transfert.

(3) Sans préjudice des dispositions du paragraphe (1), la Commission peut autoriser, sur la base d'une demande dûment motivée, un transfert ou un ensemble de transferts de données à caractère personnel vers un Etat non membre de l'Union européenne 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, 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.

(4) Quiconque effectue un transfert de données vers un pays tiers en violation des dispositions des paragraphes (2) et (3) est puni d'un emprisonnement de huit jours à un an et d'une amende de 10.001 à 5.000.000 LUF, ou d'une de ces peines seulement.

Art. 20. ***Information réciproque***

(1) La Commission nationale pour la protection des données informe le ministre compétent en la matière de toute décision prise en application de l'article 18, paragraphes (3) et (4) et de l'article 19 paragraphes (1) et (2). Le ministre en informe la Commission européenne.

(2) Le ministre compétent en la matière informe la Commission de toute décision relative au niveau de protection d'un Etat non membre de l'Union européenne prise par la Commission européenne.

Chapitre V. *Confidentialité et securité des traitements*

Art. 21. ***Confidentialité des traitements***

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***

(1) Le responsable du traitement doit mettre en oeuvre toutes les mesures techniques et d'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. Ces mesures font l'objet d'un examen annuel dont le résultat est communiqué à la Commission.

(2) Lorsque le traitement est mis en oeuvre 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 de veiller au respect de ces mesures.

(3) Tout traitement effectué pour compte doit être régi par un contrat ou un acte juridique 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;

(b) les obligations visées au présent article incombent également à celui-ci.

(4) Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures visées au présent article sont consignés par écrit.

Art. 23. ***Mesures de sécurité particulières***

Compte tenu du risque d'atteinte à la vie privée, ainsi que de l'état de l'art et des coûts liés à leur mise en oeuvre, 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 et toute personne qui exerce des fonctions auprès de la Commission 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 mandat.

(2) Le chargé de la protection des données agissant dans le cadre de l'accomplissement de ses missions, ne peut opposer à la Commission le secret professionnel auquel il est soumis.

(3) Le prestataire de service de certification ne peut opposer à la Commission le secret professionnel auquel il est soumis conformément à l'article 19 de la loi du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93 du 13 décembre 1999 relative à un cadre communautaire pour les signatures électroniques, la directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE du 20 mai 1997 concernant la vente à distance des biens et des services autres que les services financiers.

(4) Le responsable du traitement agissant dans le cadre de l'accomplissement de ses missions tel que visé à l'article 7 paragraphe (1), ne peut opposer à la Commission le secret professionnel auquel il est soumis.

Art. 25. ***Sanctions relatives à la confidentialité 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 10.001 à 3.000.000 LUF, ou d'une de ces peines seulement.

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 ou son représentant doit fournir à la personne concernée, au plus tard lors de la collecte, 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 du traitement auquel les données sont destinées;

(c) toute autre information supplémentaire telle que:
- les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
- le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse;
- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;
- la durée de conservation des données.

(2) Lorsque la collecte des données se fait moyennant formulaire ou questionnaire, quel que soit son support ou moyennant des documents qui servent de base à la collecte des données, ils doivent contenir les informations visées au paragraphe (1).

(3) Lorsque les données n'ont pas été collectées auprès de la personne concernée, le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée, 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 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;
- la durée de conservation des données.

(4) Quiconque contrevient aux dispositions de cet article est puni d'un emprisonnement de huit jours à un an et d'une amende de 10.001 à 5.000.000 LUF, ou d'une de ces peines seulement.

Art. 27. ***Exceptions au droit à l'information de la personne concernée***

(1) L'article 26 paragraphes (1) et (3) ne s'applique pas lorsque le traitement est nécessaire pour sauvegarder:

(a) la sûreté de l'Etat;

(b) la défense;

(c) la sécurité publique;

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

(e) un intérêt économique ou financier important de l'Etat ou de l'Union européenne, en particulier dans les domaines monétaire, budgétaire et fiscal;

(f) la protection de la personne concernée ou des droits et libertés d'autrui.

(2) Les dispositions de l'article 26 sont susceptibles de dérogations lors de la collecte de données dans les conditions prévues à l'article 9 paragraphe (1) (c).

(3) Les dispositions de l'article 26 paragraphes (1) et (3) 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 10.001 à 5.000.000 LUF, ou d'une de ces peines seulement.

Art. 28. ***Droit d'accès***

(1) A condition de prouver son/leur identité, la personne concernée, ou ses ayants droit justifiant d'un intérêt légitime, peu(ven)t obtenir à sa/leur demande auprès du responsable du traitement, ou de son représentant sans contrainte, 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 paragraphe (1).

(2) Celui qui entrave 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 10.001 à 5.000.000 LUF, ou d'une de ces peines seulement.

(3) Le patient a un droit d'accès aux données le concernant et collectées par son médecin. Le droit d'accès peut être exercé par le patient lui-même ou par l'intermédiaire d'un médecin qu'il désigne. En cas d'incapacité de la personne concernée, le droit d'accès peut être exercé par ses ayants droit.

(4) Toute personne a un droit d'accès aux données la concernant et utilisées aux fins d'un traitement mis en oeuvre dans le cadre de la liberté d'expression tel que prévu à l'article 9. Aussi longtemps que les données auxquelles l'accès est demandé n'ont pas été publiées, la communication de ces données, ainsi que toute information disponible sur leur origine ne peut se faire que par l'intermédiaire de la Commission qui opère conformément à l'article 9, paragraphe (3) de la présente loi.

(5) Selon le cas, le responsable du traitement ou son représentant 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 l'interdiction temporaire ou définitive du traitement ou la destruction des données.

(6) 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 qui procède aux vérifications nécessaires.

(7) Toute rectification, tout effacement ou verrouillage effectué conformément au paragraphe (5) sera notifié sans délai par le responsable du traitement ou son représentant aux destinataires auxquels les données ont été communiquées, à moins que cela ne s'avère impossible.

(8) Sans préjudice de la sanction prévue au paragraphe (5), quiconque contrevient aux dispositions de cet article ou quiconque prend 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 10.001 à 5.000.000 LUF, 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;

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

(e) un intérêt économique ou financier important de l'Etat ou de l'Union européenne, en particulier 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 et que la mesure d'exception est prise conformément à l'article 28 paragraphe (4).

(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 à caractère personnel 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.

(3) 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.

(4) En cas de limitation de l'exercice du droit d'accès de la personne concernée, le droit d'accès est exercé par la Commission 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 peut communiquer à la personne concernée le résultat de ses investigations, sans toutefois mettre en danger la ou les finalités des traitements en question.

(5) Quiconque contrevient à la disposition du paragraphe (3) qui précède est puni d'un emprisonnement de huit jours à un an et d'une amende de 10.001 à 5.000.000 LUF ou d'une de ces peines seulement.

Art. 30. ***Droit d'opposition de la personne concernée***

Toute personne concernée a le droit:

(1) 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 oeuvre par le responsable du traitement ne peut pas porter sur ces données;

(2) de s'opposer, sur demande et gratuitement, au traitement la concernant envisagé par le responsable du traitement 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;

(3) 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;

(4) Quiconque contrevient aux dispositions de cet article est puni d'un emprisonnement de huit jours à un an et d'une amende de 10.001 à 3.000.000 LUF ou d'une de ces peines seulement.

Art. 31. ***Décisions individuelles automatisées***

(1) Toute personne a le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité.

(2) Cependant, une personne peut être soumise à une décision telle que visée au paragraphe (1) si une telle 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. *Responsabilité et recours*

Art. 32. *Généralités*

Sans préjudice d'un recours devant la Commission et des actions en responsabilité prévues par le droit commun, toute personne dispose d'un recours juridictionnel tel que prévu ci-après.

Art. 33. *Recours devant la Chambre du Conseil*

(1) En cas de mise en oeuvre d'un traitement en violation des formalités prévues par la présente loi et relatives à la publicité, à la procédure de notification ou d'autorisation préalable, le Procureur d'Etat, une partie lésée ou la Commission pourront demander par voie de requête auprès de la chambre du conseil du tribunal d'arrondissement du lieu où le traitement est mis en oeuvre la suspension provisoire de l'activité de la personne physique ou morale, de l'entreprise ou de l'organisme responsable du traitement, ceci pouvant entraîner la fermeture provisoire de l'établissement du responsable du traitement lorsque sa seule activité est de traiter des données à caractère personnel.

(2) La requête notifiée au responsable du traitement au moins vingt-quatre heures à l'avance, par envoi recommandé avec accusé de réception, est déposée au greffe de la juridiction appelée à statuer. Cette requête indique le jour, l'heure et le lieu de la comparution devant la chambre du conseil.

(3) Il est statué d'urgence et au plus tard dans les trois jours du dépôt, le ministère public ainsi que les parties entendus en leurs explications orales.

(4) Si la chambre du conseil constate l'existence d'indices suffisants indiquant que le traitement est mis en oeuvre en violation des formalités visées au paragraphe (1), elle prononce la suspension provisoire de l'activité, ou le cas échéant, la fermeture provisoire de l'établissement du responsable du traitement.

(5) La décision de suspension provisoire d'activité ou de fermeture provisoire d'établissement produit ses effets aussi longtemps que les formalités en violation desquelles le traitement a été mis en oeuvre ne sont pas réalisées.

(6) L'ordonnance de la chambre du conseil est susceptible d'appel devant la chambre du conseil de la Cour d'Appel.

(7) L'appel est consigné sur un registre tenu à cet effet au greffe du tribunal dont relève la chambre du conseil. Il doit être formé dans un délai de trois jours, qui court contre le Procureur d'Etat à compter du jour de l'ordonnance et contre les autres parties en cause à compter du jour de la notification par envoi recommandé avec accusé de réception qui doit être faite dans les vingt-quatre heures de l'ordonnance.

(8) Le greffier avertit les autres parties de la déclaration d'appel dans les vingt-quatre heures de la consignation sur le registre.

(9) L'audience de la chambre du conseil de la Cour d'Appel n'est pas publique.

Le responsable du traitement en cause, la partie civile, la Commission ou toute autre partie en cause ou leurs conseils que le greffier avertit au plus tard trois jours avant les jours et heures de l'audience, ont seuls le droit d'y assister, de fournir tels mémoires et de faire telles réquisitions verbales ou écrites qu'ils jugent convenables.

Les formalités du présent paragraphe sont à observer sous peine de nullité, sauf si la personne responsable du traitement, la partie civile, la Commission ou toutes les autres parties en cause y ont renoncé.

Le responsable du traitement en cause ou son conseil a toujours la parole en dernier lieu.

(10) Les notifications et avertissements se font par envoi recommandé avec accusé de réception. Les pièces sont transmises par le Procureur d'Etat au Procureur Général d'Etat, à l'exception des pièces à conviction qui restent au greffe du tribunal d'arrondissement.

(11) Le droit d'appel appartient également au Procureur Général d'Etat, qui dispose à cet effet d'un délai de cinq jours à partir de la date de l'ordonnance.

Cet appel peut être formé par déclaration ou notification au greffe du tribunal dont relève la chambre du conseil. Le greffier en avertit immédiatement les parties.

(12) La décision de suspension provisoire d'activité ou de fermeture provisoire d'établissement prononcée par une chambre du conseil est exécutoire par provision et nonobstant tout recours exercé contre elle.

(13) Tout manquement à l'ordonnance d'une chambre du Conseil est puni d'un emprisonnement de huit jours à six mois et d'une amende de 10.001 à 3.000.000 LUF, ou d'une de ces peines seulement.

Chapitre VIII. *Contrôle et surveillance de l'application de la loi*

Art. 34. *Missions et pouvoirs de la Commission Nationale pour la Protection des Données*

(1) Il est institué une autorité de contrôle dénommée „Commission Nationale pour la Protection des Données" dénommée dans la présente loi „la Commission", chargée de contrôler et de vérifier si les données à caractère personnel 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 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 les déficiences ou abus qui ne sont pas spécifiquement visés par les dispositions légales, réglementaires et administratives existantes. Elle publiera son rapport annuel.

(3) Les missions de la Commission 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 oeuvre 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 oeuvre des traitements soumis au régime de l'article 14 de la présente loi;

(e) émettre un avis préalable à l'adoption des mesures réglementaires ou administratives et être consultée préalablement à l'adoption de tout texte de loi portant création d'un traitement, ainsi que de tout projet de modification de ces mesures ou texte de loi, l'avis est publié dans les documents parlementaires et dans le rapport de la Commission;

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

(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 peut être saisie par toute personne ou par une association la représentant, d'une demande relative au respect de ses droits et libertés fondamentaux à l'égard d'un traitement. La personne concernée est informée des suites réservées à sa requête.

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

(6) Dans le cadre de la présente loi, la Commission 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 où a lieu le traitement ainsi qu'aux données faisant l'objet du traitement et procède aux vérifications nécessaires.

(7) La Commission 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.

(8) La Commission coopère avec ses homologues que sont les autorités de contrôle instituées dans les autres Etats membres de l'Union européenne, notamment en échangeant toute information nécessaire à l'accomplissement de leurs missions respectives ou en exerçant ses pouvoirs sur demande d'une de celles-ci.

(9) La Commission 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, de même qu'à toute autorité de contrôle commune instituée par des instruments juridiques internationaux.

(10) Quiconque empêche ou entrave volontairement, de quelque manière que ce soit, l'accomplissement des missions incombant à la Commission, est puni d'un emprisonnement de huit jours à un an et d'une amende de 10.001 à 5.000.000 LUF, ou d'une de ces peines seulement. Est considéré comme empêchant ou entravant volontairement l'accomplissement des missions incombant à la Commission, le refus opposé à ses membres de donner accès aux locaux où a lieu un traitement aux données faisant l'objet d'un traitement ou de communiquer tous renseignements et documents demandés.

Art. 35. ***Sanctions administratives***

(1) Sans préjudice des poursuites pénales éventuelles et des peines d'emprisonnement et/ou des amendes prévues par la présente loi, le responsable du traitement, son représentant ou le cas échéant le sous-traitant dont les traitements sont soumis au contrôle de la Commission, peuvent être frappés par celle-ci, après une procédure contradictoire, d'une amende d'ordre qui ne peut dépasser 10.000.000 francs lorsqu'il s'agit d'une personne morale et de 500.000 francs lorsqu'il s'agit d'une personne physique pour l'une des infractions commises à la présente loi et/ou à ses règlements d'exécution ainsi qu'aux instructions de la Commission. En cas de récidive, le montant de l'amende d'ordre sera doublé.

(2) En outre, la Commission peut prononcer soit en sus de l'amende d'ordre l'une ou l'autre des sanctions disciplinaires suivantes:

(a) avertir ou admonester le responsable du traitement;

(b) verrouiller, effacer ou détruire des données faisant l'objet d'un traitement contraire aux dispositions de la présente loi et/ou de ses règlements d'exécution;

(c) interdire temporairement ou définitivement un traitement contraire aux dispositions de la présente loi et/ou à ses règlements d'exécution;

(d) ordonner l'insertion intégrale ou par extraits de la décision d'interdiction dans un ou plusieurs journaux quotidiens aux frais de la personne condamnée;

(3) Les sanctions précitées seront prises dans le respect du principe du contradictoire et des droits de la défense. Un règlement grand-ducal peut déterminer les modalités de la procédure contradictoire.

Art. 36. ***Composition de la Commission Nationale pour la Protection des Données***

(1) La Commission est une autorité indépendante qui prend la forme d'un établissement public doté de la personnalité juridique, d'une autonomie administrative et financière. Son siège est établi à Luxembourg-ville.

(2) La Commission est composée de trois membres effectifs et de trois membres suppléants dont un président et un vice-président nommés par le Grand-Duc pour un terme de six ans renouvelable une fois.

(3) Le Grand-Duc nommera les membres sur proposition du Gouvernement en conseil. Le Gouvernement en conseil proposera comme membre effectif au moins un juriste et un informaticien justifiant d'une formation universitaire accomplie.

Les membres de la Commission sont proposés pour leur compétence professionnelle reconnue dans leur(s) matière(s) respective(s).

(4) Les membres de la Commission 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 à caractère personnel.

(5) Si, en cours de mandat un membre de la Commission cesse d'exercer ses fonctions, le mandat de son successeur est limité à la période restant à courir. Leur mandat cesse de plein droit dès l'atteinte de la limite d'âge de soixante-cinq ans.

(6) Avant d'entrer en fonction, les membres de la Commission prêtent entre les mains du président de la Commission 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."

Art. 37. ***Fonctionnement de la Commission Nationale pour la Protection des Données***

(1) La Commission 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 B.

(2) Sous réserve des dispositions de la présente loi, le règlement intérieur fixe:

(a) les règles de procédure applicables devant la Commission

(b) les conditions de fonctionnement de la Commission

(c) les modalités de désignation du président et du vice-président

(d) l'organisation des services de la Commission.

(3) Les membres effectifs de la Commission sont convoqués par le président. La convocation est de droit à la demande de deux membres effectifs. La convocation précise l'ordre du jour.

(4) La Commission ne peut valablement délibérer que si la majorité de ses membres en exercice présents ou suppléés participe à la séance.

(5) La Commission constate préalablement à chaque délibération les conflits d'intérêts opposables à ses membres et suspend leur droit de vote jusqu'à la délibération suivante.

(6) Les délibérations de la Commission sont prises à la majorité absolue des membres présents. Toutefois, sont prises, à la majorité d'au moins deux voix les délibérations suivantes:

(a) l'adoption et la modification du règlement intérieur;

(b) l'émission d'un avis ou l'octroi d'une autorisation.

(7) Le Gouvernement en conseil ayant proposé à la nomination un membre de la Commission peut proposer sa révocation au Grand-Duc après avis conforme de la Commission pris à la majorité des membres présents.

(8) Dans l'exercice de leurs fonctions, les membres et les suppléants de la Commission ne reçoivent d'instruction d'aucune autorité.

Art. 38. ***Statut des membres et agents de la Commission Nationale pour la Protection des Données***

(1) La Commission est assistée dans l'exercice de ses missions par des agents nommés et placés sous son autorité.

(2) Les membres et agents de la Commission sont des employés privés à assimiler à des employés de l'Etat, sans préjudice des dispositions de la présente loi et de celles d'un règlement grand-ducal à prendre en matière de cadre, de rémunération et de promotion des agents de la Commission.

(3) Avant d'entrer en fonctions les agents prêtent entre les mains du président de la Commission le serment qui suit: „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."

(4) Les rémunérations et autres indemnités de tous membres, agents et employés de la Commission sont à charge de la Commission.

(5) Le cadre du personnel de la Commission pourra être complété par des employés et des ouvriers, nécessaires au bon fonctionnement, dans les limites des crédits budgétaires de la Commission.

(6) La Commission peut également faire appel à des experts externes qui sont engagés sur base d'un contrat de droit privé.

Art. 39. ***Dispositions financières***

(1) Au moment de sa création, la Commission nationale pour la protection des données bénéficie d'une dotation de X millions de francs à faire part du budget de l'Etat ainsi que d'un apport de biens mobiliers et immobiliers nécessaires au bon fonctionnement et à l'exercice de ses missions.

(2) L'exercice financier de la Commission coïncide avec l'année civile.

(3) Avant le 31 mars de chaque année, la Commission approuve son bilan de l'exercice précédent, ensemble avec son rapport de gestion. Avant le 30 septembre de chaque exercice, la Commission approuve le budget pour l'exercice à venir.

Le budget les comptes annuels et les rapports approuvés sont transmis au Conseil de Gouvernement qui décide de la décharge à donner à la Commission. La décision constatant la décharge accordée à la Commission ainsi que les comptes annuels de la Commission sont publiés au Mémorial.

(4) La Commission est autorisée à prélever la contrepartie de ses frais du personnel en service et de ses frais de fonctionnement par la redevance à percevoir telle que prévue à l'article 13 de la présente loi. Pour le solde des frais restant à couvrir, la Commission bénéficiera d'une dotation d'un montant à déterminer sur une base annuelle et à faire part du budget de l'Etat.

Art. 40. ***Le chargé de la protection des données***

(1) Tout responsable de traitement peut, dans le cadre de l'article 12 paragraphe (2) (a), désigner un chargé de la protection des données, dont il communique l'identité à la Commission.

(2) Les missions du chargé de la protection des données sont les suivantes:

(a) assurer l'application des dispositions de la présente loi et de ses règlements d'exécution aux traitements qu'il est appelé à surveiller;

(b) tenir un registre des traitements effectués par le responsable du traitement identique à celui tenu par la Commission quant à son contenu et son fonctionnement afin de garantir que ces traitements ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées.

(3) 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.

(4) 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:

(a) il ne connaît aucun lien de subordination vis-à-vis du responsable du traitement et ne peut être lié au responsable du traitement par un contrat de travail:

(b) il ne peut subir de désavantage du fait de l'exécution de ses missions;

(c) il ne peut être révoqué pour des raisons liées à l'exercice de ses missions, hormis le cas de la violation de ses obligations légales et/ou conventionnelles.

(5) Le chargé de la protection consulte la Commission en cas de doute quant à la conformité à la présente loi d'un traitement mis en oeuvre 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, ou celles pouvant exercer cette activité de plein droit.

(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 ainsi que d'assises financières d'une valeur de quinze millions de francs au moins. L'agrément est délivré par la Commission.

(8) Les membres inscrits dans une des professions réglementées suivantes peuvent immédiatement exercer l'activité de chargé de la protection des données: avocat, 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 vérifie les qualités de tout chargé de la protection des données qu'il soit agréé ou membre d'une des professions réglementées visées au paragraphe qui précède, en examinant son activité professionnelle antérieure à la désignation, et en organisant un contrôle continu et/ou en l'examinant sur sa connaissance de la matière.

La Commission peut s'opposer à tout moment à la désignation du chargé de la protection des données lorsqu'il:

– ne présente pas les qualités requises pour la fonction de chargé de la protection des données;

ou

– est d'ores et déjà en relation avec le responsable du traitement dans le cadre d'autres activités que celle du traitement des données à caractère personnel et que cette relation fait naître un conflit d'intérêts limitant son indépendance.

En cas d'opposition de la Commission, le responsable du traitement dispose de trois jours pour désigner un nouveau chargé de la protection des données.

(10) La Commission définit les modalités du contrôle continu des qualités requises à la fonction de chargé de la protection des données en organisant des formations à valider.

(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.

Chapitre IX. *Dispositions spécifiques, transitoires et finales*

Art. 41. *Dispositions spécifiques*

(1) Les autorités compétentes visées aux articles 88-1 à 88-4 du code d'instruction criminelle, le procureur d'Etat agissant en matière de flagrant délit ou toute personne agissant dans le cadre de la sauvegarde de la vie humaine, accède de plein droit, sur requête et par l'intermédiaire de l'Institut luxembourgeois de régulation (ILR) aux données concernant les abonnés des opérateurs de télécommunications et/ou des services postaux et/ou de leurs fournisseurs de services. A ces fins les opérateurs et/ou leurs fournisseurs de services mettent d'office et gratuitement à disposition de l'ILR les données relatives aux abonnés et à leurs services. Les données doivent être mises à jour 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 télécommunications et services postaux pour lesquels les opérateurs et/ou fournisseurs de services doivent mettre à disposition les données ainsi que la nature, le format et les modalités de mises à disposition des données dans le cadre de l'article 41 paragraphe (1).

(2) 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 ainsi que celles prises en matière de flagrant délit;
– à la sauvegarde de la vie de la personne concernée (abonné concerné) ou d'une tierce personne.

Dans le cadre de la sauvegarde de la vie, l'accès de plein droit est défini conformément à un code de conduite approuvé par la Commission et déterminant les personnes autorisées.

(3) Si une requête est introduite dans le cadre des mesures spéciales de surveillance telles que prévues aux articles 88-1 à 88-4 du code d'instruction criminelle ainsi que dans le cadre des mesures prises en matière de flagrant délit, l'ILR l'exécute dans un délai de 24 heures dès sa réception. Si une requête est introduite en vue de l'accomplissement d'une mission de sauvegarde de la vie humaine, l'ILR l'exécute immédiatement dès réception de celle-ci. Un ou plusieurs fonctionnaires de l'ILR, désignés à ces fins, sont chargés de l'exécution des requêtes auprès des opérateurs et/ou de leurs fournisseurs de services prévus à l'article 41 paragraphe (1).

(4) L'ILR peut entièrement automatiser cette procédure suite à l'autorisation de la Commission. La Commission vérifiera en particulier la sécurisation du système informatique utilisé. Cette automatisation permettra l'accès par voie électronique et sans qu'une intervention manuelle soit requise.

(5) Les données mises à disposition dans le cadre de l'article 41 paragraphe (1) ne peuvent faire l'objet d'un nouveau traitement et être ainsi dépourvues de leur finalité primaire. L'ILR tient un registre des requêtes qui fera l'objet d'une communication semestrielle à la Commission.

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 peut permettre que les données conservées uniquement à des fins de recherche historiques soient dispensées de respecter le paragraphe (1).

Art. 43. ***Mise en oeuvre des dispositions transitoires***

(1) La Commission établira le schéma de notification prévu à l'article 13 paragraphe (3), dans les trois 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.

(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 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. Dans ce cas, le délai prévu au paragraphe (2) qui précède est de rigueur.

(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***

La loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, telle qu'elle a été modifiée par les lois des 19 novembre 1987, 30 septembre 1992, 1er octobre 1992 et 9 août 1993 et ses règlements d'exécution sont abrogés.

Art. 45. ***Entrée en vigueur***

La présente loi entre en vigueur le premier jour du mois qui suit sa publication au Mémorial.

*

COMMENTAIRE DES ARTICLES

Chapitre I. *Dispositions générales*

ad Article 1er

Les technologies de l'information facilitent considérablement le traitement et l'échange des données, et le volume et la rapidité des flux transfrontaliers de données ne cessent de s'accroître. Dans ce contexte, le présent article met en place un équilibre entre la protection des droits et libertés fondamentaux des personnes concernées et la libre circulation de ces données.

Bien que la protection des personnes morales ne soit pas explicitement prévue par la Directive, le présent projet de loi de transposition énonce qu'un traitement illicite ou abusif de données à caractère personnel, peut-être constitutif d'une atteinte non seulement aux libertés et droits fondamentaux des personnes physiques, mais également aux intérêts légitimes des personnes morales.[1]

Abstraction faite qu'on ne peut parler d'une „vie privée" des personnes morales, la pratique montre que, sauf dans des cas exceptionnels, et notamment celui des statistiques, les données „à caractère personnel" concernant les personnes morales sont aussi protégées contre des abus de traitement par d'autres textes de loi, telles que par exemple les règles de droit commercial.

Il existe une double raison de maintenir la référence aux personnes morales telle que prévue dans la loi du 31 mars 1979:

1. Reconnaître aux personnes morales certains droits accordés par la Directive aux personnes physiques, tel que le droit d'accès et le droit de rectification, leur permettre de protéger leur image informationnelle et éviter que des décisions soient prises à l'encontre des personnes morales sur la seule base d'informations incorrectes, incomplètes ou erronées.
2. Le droit d'accès est important dans la mesure où des personnes physiques peuvent être affectées par des mesures prises à l'égard d'une personne morale (exemple: fermeture d'une entreprise).

En effet, la prise en compte des personnes morales permet d'aborder les problèmes liés à la concurrence et au secret des affaires dans la mesure où les traitements de données commerciales (fichiers „clients ", fichiers „fournisseurs " etc.) ont une importance stratégique considérable pour la plupart des entreprises.

La reconnaissance de certains droits, comme le droit d'accès, permet aux entreprises de pouvoir protéger leur image informationnelle vis-à-vis des responsables de traitement et d'éviter que leur soit appliqué un traitement inadéquat en raison de données fausses.

Une autre justification tient au fait qu'il est fréquent que l'on protège indirectement les personnes physiques à travers des données concernant les personnes morales.

La protection plus générale de certaines libertés fondamentales (telles que, par exemple, la liberté d'association) s'opère notamment à travers la protection de personnes morales du type associations d'utilité publique sans but lucratif (par exemple).

Par conséquent, afin de combler d'éventuelles lacunes qui pourraient se créer dans l'une ou dans l'autre situation, la présente loi s'applique aux personnes morales dans le but de faire respecter leurs intérêts légalement protégés.

La référence à l'intérêt légalement protégé (article 1er) permet de prévenir l'utilisation de certains droits tirés de la présente loi à des fins illégitimes, par exemple, si une entreprise se servait de son droit d'accès pour connaître la stratégie commerciale d'une entreprise concurrente.

ad Article 2

L'article 2 reprend in extenso les définitions utilisées dans la directive 95/46/CE et ajoute celles de l'„interconnexion"(e) du „ministre" (f), de la „surveillance" (h) issue elle du *projet de recommandation sur la protection des données à caractère personnel collectées et traitées à des fins de surveillance (Conseil de l'Europe, mai 99, réf CJ-PD-GTNT (98)4rev2)* ainsi que celle du „code de conduite" (m). La définition relative au „fichier de données à caractère personnel (d) a été élargie par rapport à celle de la directive" (cf. infra).

---

1) La protection de la „vie privée" des personnes morales était déjà garantie par la loi du 31 mars 1979.

Ainsi, „aux fins de la présente loi“, on entend par **(a) „donnée à caractère personnel“**, toute information relative à une personne qui est identifiée ou qui est identifiable („personne concernée“). La définition précise qu'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.

Cela implique que des données codées peuvent être des données à caractère personnel. Il s'agit dans ce cas de données ayant subi un processus permettant de les rendre anonymes en vue de la réalisation de finalités historiques, statistiques ou scientifiques. En effet, à partir du moment où un intermédiaire quelconque est apte à faire le lien entre une donnée et une personne concernée, cette donnée, certes codée, est certainement une donnée à caractère personnel.

Hormis l'utilisation du qualificatif „génétique“, il s'agit de la définition donnée par la Directive 95/46/CE, au sujet de laquelle Marie-Hélène Boulanger, Cécile de Terwangne, Thierry Léonard, Sophie Louveaux, Damien Moreau et Yves Poullet, dans leur dossier „La protection des données à caractère personnel en droit communautaire“, paru dans le Journal des Tribunaux – Droit européen, juin 1997, font le commentaire suivant: *„La notion d'information n'est pas définie. Dès lors, elle n'est soumise à aucune exigence de forme particulière. Une information écrite, chiffrée, mais également présente dans une image ou un son sont constitutives de données.“* On a donc mentionné qu'une donnée est personnelle, indépendamment de son support ou de sa forme.

Que les informations *„présentes dans une image ou un son sont constitutives de données“* (à caractère personnel), est par ailleurs souligné dans le considérant (14) de la Directive: *„considérant que, compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives aux personnes physiques, la présente Directive est appelée à s'appliquer aux traitements portant sur ces données.“* Cela signifie que tout traitement de sons et/ou d'images, par quelque moyen que ce soit (enregistrement audio ou vidéo, notamment par vidéosurveillance, multimédia etc.) rentre dans le champ d'application de la loi du moment que ces sons et images peuvent être attribués à une personne identifiée ou identifiable.

Selon les auteurs du dossier cité ci-dessus, une personne *„est réputée identifiable, dès lors qu'une possibilité existe de l'identifier directement ou indirectement notamment par un numéro de téléphone, de plaque d'immatriculation de voiture, de sécurité sociale ou de passeport. Le texte précise par ailleurs qu'une personne peut être identifiée par référence à un ou plusieurs éléments spécifiques propres à son identité sous toutes ses formes (âge, fonction professionnelle, adresse, etc.) même empreinte* digitale ou gène.

Se pose forcément le problème de savoir quand on n'est pas ou plus en présence de données à caractère personnel, respectivement quand on est en présence de données anonymes, dont le traitement ne rentre pas dans le champ d'application de la loi.

Ici les auteurs précités considèrent que *„dès lors que, techniquement, in abstracto, un moyen existe de rendre les personnes concernées identifiables, elles sont réputées telles par la définition. Le caractère identifiable apparaît alors comme relatif eu égard aux possibilités d'identification du ou des responsables“* [du traitement]. *„Il revient (…) à la personne qui traite les données et qui considère ne pas devoir respecter les principes protecteurs, de rapporter la preuve du caractère anonyme de celles-ci dans son chef; en présentant toute garantie utile quant à la conservation du caractère anonyme des données (…).“*

Le considérant (26) de la Directive 95/46/CE précise *„que, pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en oeuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne“*.

La définition sub **(b) „personne concernée“** précise que la loi vise le respect des libertés et droits fondamentaux des personnes physiques, mais également, le cas échéant, le respect des intérêts légitimes des personnes morales, publiques ou privées, et des groupements de fait.[1]

---

1) La Directive 97/66/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications protège les personnes morales dans la mesure où elles auraient un intérêt légitime à être protégées pour elles-mêmes (voir note No 30, ouvrage précité, page 124).

La définition sub **(c) „traitement de données à caractère personnel“** remplace celle de la „banque de données nominatives“ définie par la loi de 1979, notion surannée, alors que ce n'est pas tant l'enregistrement de données à caractère personnel dans une banque de données ou dans un fichier qui pourrait être à l'origine d'abus, mais bien le traitement de ces données. D'autre part, la multiplication des réseaux a rendu de plus en plus difficile la localisation d'un fichier ainsi que son lieu d'exploitation. Enfin, on peut noter qu'aujourd'hui un traitement peut exister sans prendre la forme d'un fichier. Les données peuvent en effet être entièrement décentralisées sur le réseau Internet. Les auteurs de la Directive ont volontairement souhaité une définition extensive. Sont visées *„toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données à caractère personnel*“, opérations allant de la collecte à l'effacement ou à la destruction des données.

Ainsi, la collecte est désormais considérée comme une opération faisant partie intégrante du traitement des données. Ce qui veut dire, d'une part, que la collecte fait partie d'un traitement, et ne devrait donc pas être effectuée seule, si d'autres opérations comme l'enregistrement, la conservation ou l'utilisation des données pour une ou des finalités déterminées ne sont pas susceptibles de la suivre. Ce qui veut dire, d'autre part, que si la collecte de données à caractère personnel devait, pour une raison ou une autre, être effectuée de façon isolée dans le temps, sans être rattachée immédiatement à d'autres opérations, elle doit obéir aux dispositions afférentes de la loi, et notamment à celle énoncée à l'article 4, paragraphe (1) sous (a).

Ainsi, une collecte de données à caractère personnel „en prévision“ sera dorénavant exclue, étant donné qu'elle sera illicite. Selon les auteurs précités: *„On a voulu par là reconnaître à la personne concernée une protection complète dès la saisine des données par autrui même si le traitement réel n'intervient que bien plus tard. Il a dès lors pu être jugé utile de préciser qu'une seule opération – sous-entendu la collecte – pouvait être considérée comme un traitement de façon anticipative. Ainsi, tout le processus de traitement est visé.“*

La définition de **„fichier de données à caractère personnel“ (d)** est „tout ensemble structuré ou non de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique“.

Cette définition, plus large que celle prévue dans la directive, permet d'éviter de donner l'impression qu'on ne protège que les données reprises dans les „fichiers informatiques classiques“ mais qu'elle inclut toutes les formes d'enregistrement de données possibles (ex. formes structurées: systèmes de gestion de bases de données qui attribuent une signification très précise à chaque donnée (colonne d'une table), forme moins structurée: dans les logiciels de traitement de texte qui permettent de gérer des données (dans les tableaux), forme non structurée: dans les logiciels de traitement de texte).

Sub **(e), „l'interconnexion“** est définie comme une forme de traitement qui consiste en la corrélation de données à caractère personnel traitées pour une finalité précise avec des données à caractère personnel traitées pour une autre finalité, que ce soit par le même responsable du traitement ou par des responsables de traitement différents. Cette définition innove par rapport à la loi de 1979 dans la mesure où elle permet d'interconnecter des banques de données même celles „relevant de l'Etat “ et ainsi de tenir compte d'un besoin reconnu depuis longtemps.

Sub **(f) „le ministre“**; cette définition n'exige pas d'observations particulières.

Sub **(g) le „responsable du traitement“** est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Elle désigne „la personne responsable des choix qui président à la définition et à la mise en oeuvre des traitements. Ces choix sont relatifs aux finalités et aux moyens utilisés. Si différentes personnes ou autorités déterminent conjointement ces éléments, elles seront chacune considérées comme responsables“ (auteurs précités). La définition précise que lorsque les finalités et les moyens du traitement sont déterminés par des dispositions légales, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par ces dispositions légales.

Le responsable du traitement *„doit cependant être distingué des personnes qui procèdent aux opérations de traitement en conformité à ses instructions. Celui-ci peut ainsi faire traiter les données par les membres de son personnel ou par un sous-traitant, personne juridiquement distincte mais agissant pour son compte*“ (auteurs précités).

La définition, **sub (i), du „sous-traitant“** remplace celle de „gestionnaire“, définie par la loi du 31 mars 1979 comme la „personne qui tient effectivement la banque en appliquant aux données à caractère personnel des traitements automatiques“.

La **surveillance sub (h)** est une notion centrale dans le cadre de l'activité de prévention de la criminalité. Elle est également permise sur le lieu de travail. Cette définition reprend utilement celle proposée dans le projet de recommandation du Conseil de l'Europe de mai 1999 (CJ-PD-GTNT (98) 4rev2). Cette définition est suffisamment large pour appréhender l'ensemble des techniques de surveillance y compris la vidéosurveillance, la surveillance électronique et informatique.

La définition de **„tiers", sub (j),** souligne utilement:

– d'abord, que par „tiers" on désigne les personnes, quel que soit leur statut, autres que la personne concernée, d'une part, le responsable du traitement et le sous-traitant, de l'autre;
– ensuite, que les personnes qui sont placées sous l'autorité directe du responsable du traitement ou du sous-traitant et qui par là sont habilitées à traiter les données à caractère personnel, ne sont pas non plus à considérer comme des tiers.

Pour le secteur public une précision de la notion de tiers s'impose au regard de la diversité des organes publics existants. Ainsi, on entend par tiers un ministère, une administration, un établissement public, une commune ou un service public autre que celui qui est le responsable du traitement ou son sous-traitant.

Sub (k) définit le „destinataire" comme étant la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers[1]; les autorités qui sont susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière[2] ne sont toutefois pas considérées comme des destinataires.

La loi du 31 mars 1979 consacrait l'autorisation préalable de la création et de l'exploitation d'une banque de données comme unique condition de licéité d'un traitement de données à caractère personnel. L'objet de la présente loi étant de remplacer, pour la majorité des traitements, l'ancienne condition de licéité par un certain nombre de nouvelles conditions, telles que prévues par la Directive 95/46/CE, et notamment celle du **„consentement de la personne concernée", sub (l).** Il s'agit en l'occurrence de toute manifestation de volonté non équivoque voire expresse, libre, spécifique et informée par laquelle la personne concernée, ou son mandaté accepte que des données à caractère personnel le concernant fassent l'objet d'un traitement.

L'appréciation critique donnée au consentement „libre" est tout à fait pertinente. Ainsi dans une situation économique qui met en relation une personne faible (la personne concernée) et une personne dominante (le responsable du traitement), comme, par exemple, lors de l'obligation de contracter un prêt bancaire ou une assurance-vie, peut-il s'avérer fort probable que le consentement de la personne concernée n'est pas forcément libre, alors qu'il lui est demandé de fournir telle ou telle donnée à caractère personnel „nécessaire" pour que la conclusion du contrat lui entraînera la prestation de service nécessitée puisse avoir lieu. De ce fait, le consentement de la personne concernée est une condition primordiale de licéité d'un traitement de données à caractère personnel.

Outre le caractère libre, *„le consentement doit également être spécifique. Il ne peut avoir un objet général, mais doit porter sur des traitements précisément définis notamment quant aux finalités poursuivies par des responsables déterminés.*

Le consentement doit enfin être informé. Le responsable du traitement doit donc transmettre à la personne concernée toute information nécessaire à l'analyse du risque particulier que représente le traitement envisagé pour ses droits et libertés. A cet égard, l'information reçue par la personne concernée au moment de la collecte semble constituer un minimum" (ibidem).

La définition du **„code de conduite" (m)** est de nature mixte et trouve sa source dans l'article 27 paragraphe 2 de la Directive 95/46/CE. Une telle définition est rendue nécessaire par l'absence de précédent de ce type anglo-saxon de régulation dans notre système juridique. Il a donc fallu définir et fonder une notion nouvelle ce qui ne va pas sans édicter un minimum de règles. La seule entorse à la summa diviso entre le corps législatif du texte de loi et ses définitions porte sur le caractère facultatif de

1 Le destinataire peut être „simple" comme c'est par exemple le cas de l'audit interne ou bien être „tiers" comme c'est par exemple le cas d'un audit externe.

2 Il s'agit, par exemple, des agents du fisc ou encore de ceux de la sécurité sociale spécialement habilités pour opérer des contrôles sur les informations traitées. Ne seront pas considérées comme destinataires les autorités publiques dans le cadre d'enquêtes policières ou judiciaires, de même que les organismes intervenant dans le cadre de commissions rogatoires internationales.

sa soumission pour approbation. Cette précision ne gâche en rien la définition car elle définit clairement la limite du mécanisme ainsi institué.

Le code de conduite est un document visant dans le cadre de l'„autorégulation" à améliorer la clarté et l'application de la loi en tenant compte des spécificités de certains secteurs. On vise par exemple le secteur financier et les professions libérales. Sa valeur juridique dépendra de son intégration dans les réglementations et autres codes déontologiques réglementant l'exercice de certaines professions (ex. avocats, médecins, journalistes etc.).

Les définitions (o) et (p) n'appellent pas de commentaire particulier.

Les lettres (q) et (r) reprennent les définitions retenues par l'article 28-1, paragraphe (2) de la loi du 31 mars 1979, telle que modifiée par la loi du 1er octobre 1992, hormis la définition des données médicales dont l'insertion est prévue à l'article 6(1).

ad Article 3

La directive laisse aux Etats membres une marge d'appréciation importante quant à l'étendue du champ d'application matériel. Pour éviter tout vide juridique et en vue d'instaurer un régime juridique unifié, le projet de loi a opté pour un champ d'application large en incluant:

a) la défense, la sécurité publique, la sûreté de l'Etat et les activités de l'Etat relatives à des domaines du droit pénal etc. La Directive 95/46/CE ne distingue pas entre personne publique et personne privée mais instaure un corps de règles supranationales auxquelles sont soumis l'Etat, les communes, les établissements publics etc. La Directive n'intègre pas la défense, la sûreté, la sécurité publique ainsi que les activités de droit pénal dans son champ d'application. En revanche la loi de 1979 dans son article 12 prévoyait d'intégrer ces matières. Dans l'optique de la continuité, et afin de créer un système juridique complet, le projet de loi suit la démarche de 1979. Cette situation doit toutefois prendre en compte le particularisme de la puissance publique. Les aménagements nécessaires ont été prévus aux articles traitant de ces matières.

L'inclusion des 4 matières à savoir la défense, la sécurité publique, la sûreté de l'Etat et les activités de l'Etat relatives à des domaines du droit pénal (méthode également adoptée par la loi portugaise et en partie par la loi belge) présente l'avantage de clarifier et d'unifier le régime juridique de la protection des données tout en autorisant l'Etat à prévoir les limitations et dérogations nécessaires à l'exercice de la puissance publique. Des lois spéciales pourront en tout état de cause déroger et/ou préciser le projet de loi.

b) les sons, les images: compte tenu de l'évolution des technologies de l'information susceptibles d'accroître le flux quotidien de données, le projet de loi saisit la possibilité offerte par la directive, en s'appliquant à „toute forme de captage, de traitement et de diffusion de sons et images qui permettent d'identifier des personnes physiques ou morales" (article 3 paragraphe (4) projet de loi).

Le paragraphe (1) (champ d'application matériel) précise que le projet de loi s'applique à tout traitement, automatisé en tout ou en partie. Cela veut dire que si au moins une des opérations, dont l'ensemble constitue le traitement tel que défini à l'article 2 du présent projet, est effectuée de façon automatisée, les autres l'étant de façon „manuelle", le traitement doit être opéré en conformité avec les dispositions de la présente loi. En particulier si la collecte de données se fait de façon „manuelle" (par exemple lors de sondages moyennant formulaire ou questionnaire papier, sondages avec enregistrement audio des réponses ou sondages par téléphone), mais que par la suite les données collectées sont enregistrées sur support informatique, cette collecte doit inévitablement obéir aux dispositions du présent projet de loi. D'autre part si on copie un fichier informatisé sur papier (par exemple un listing), le traitement ultérieur de ces données à caractère personnel ne peut se faire que dans le respect des dispositions de la présente loi. En outre, le projet de loi s'applique aussi à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier tel que défini à l'article 2 sous (d).

Le paragraphe (2) (application de la loi du for) indique les différents cas où un traitement de données à caractère personnel tombe sous le champ d'application du projet de loi.

Ainsi le projet de loi s'applique-t-il si, (a) le responsable du traitement est établi sur le territoire luxembourgeois ou en un lieu où est applicable le droit luxembourgeois.

Le considérant 19 de la Directive précise:

1. la notion d'établissement stable: *„l'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel au moyen d'une installation stable"*;

2. la forme juridique de cet établissement: *„la forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante"*, car chaque établissement quel qu'il soit doit remplir *„les obligations prévues par le droit national applicable aux activités de chacun d'eux.*[1]

Dans son rapport[2] , Monsieur Guy Braibant explique que *„dans le cas où le responsable du traitement dispose de plusieurs établissements dans différents Etats membres, (…) celui-ci doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable aux activités qu'il poursuit. Chaque établissement sera donc soumis à la seule loi de l'Etat sur le territoire duquel il est implanté. Ainsi, si une entreprise française fabrique au Portugal des produits qu'elle vend en Allemagne à partir d'un établissement situé en France, les traitements de données à caractère personnel impliqués par la gestion du site de production situé au Portugal seront soumis à la loi portugaise, alors que les traitements découlant de la gestion de la clientèle allemande, effectués par l'établissement situé en France, seront soumis à la loi française"*.

L'article 3 paragraphe (2) (b) prévoit qu'un responsable du traitement qui, sans être établi sur le territoire d'un des Etats membres de l'Union européenne, recourt aux fins du traitement à des moyens automatisés ou non situés sur le territoire luxembourgeois doit respecter la présente loi. Il faut entendre le terme „moyens" de façon extensive; il s'agit de tous moyens en matériel ou en personnel. La seule exonération concerne l'utilisation de ces moyens à des fins de transit. Dans ce cas il est précisé que le responsable du traitement doit désigner dans ce cas un représentant établi sur territoire luxembourgeois qui se substitue à ses droits et obligations.

Concernant les exclusions au champ d'application (article 3, paragraphe (3)), elles sont limitées aux traitements effectués par une personne physique pour l'exercice d'activités exclusivement personnelles et domestiques.

Le considérant (12) de la Directive 95/46/CE précise qu'en l'occurrence il s'agit du *„traitement de données effectué par une personne physique (…) telles la correspondance et la tenue de répertoires d'adresses"*. Il s'ensuit que les données à caractère personnel soumises à un tel traitement ne sont pas susceptibles d'être communiquées à des tiers, sous peine d'ôter au traitement en question son caractère personnel ou domestique.

L'article 3 paragraphe (4) complète la définition de la donnée à caractère personnel et inclut en particulier le son et l'image.

L'article 3 paragraphe (5) fait entrer dans le champ d'application du projet de loi la sécurité publique, la défense, la sûreté de l'Etat, le bien-être économique lorsque celui-ci est lié à la sûreté de l'Etat et les activités relatives à des domaines du droit pénal. Ceci permet de clarifier et d'unifier le régime de la protection des données tout en autorisant l'Etat à prévoir les limitations et dérogations nécessaires à l'exercice de la puissance publique.

Certaines limitations et dérogations sont d'ores et déjà comprises dans la loi. De plus, là où la loi le prévoit, les lois actuellement en vigueur pourront déroger au régime de la protection des données. Ainsi les articles relatifs aux catégories particulières de données qualifiées de „données sensibles", aux dérogations au droit à l'information et au droit d'accès prévoient de telles dispositions.

Enfin, des lois spéciales pourront à l'avenir édicter d'autres dérogations et limitations.

---

1 Quant aux conflits de lois susceptibles d'apparaître, ils devront être réglés conformément aux régles du droit international privé et notamment par application des Conventions de Bruxelles et Lugano.

2 Guy Braibant, Données personnelles et société de l'information, Rapport au Premier Ministre, Collection des Rapports Officiels, La Documentation française, 2e trimestre 1998, page 23.

Chapitre II. *Conditions de licéité du traitement*

ad Article 4

L'article 4 paragraphe (1) reprend les dispositions de l'article 6 de la directive, impose au responsable du traitement d'entreprendre le nécessaire pour que les données à caractère personnel soient traitées **loyalement et licitement.**

La loyauté et la licéité du traitement impliquent en premier lieu que le responsable du traitement ne doit **collecter des données à caractère personnel que pour des finalités déterminées, explicites et légitimes (a)** et non pas de manière incompatible avec ces finalités. Le respect de la finalité étant le principe de base à respecter.

„La doctrine a souligné l'importance du principe de la finalité du traitement pour la protection de la vie privée. Ce principe repose sur le postulat que la menace pour la vie privée que constituent les traitements de données à caractère personnel réside davantage dans la finalité qu'ils poursuivent que dans la nature des données traitées. C'est en outre à partir de la finalité d'un traitement que tout un faisceau d'exigences est formulé quant à la nature des données enregistrées, à leur durée de conservation et à la qualité de leur destinataire" (ibidem).

Il est précisé que les données doivent être collectées pour des finalités déterminées et explicites. Alain Pipers, dans son livre „Le respect de la vie privée" paru aux Editions Politeia asbl, Bruxelles 1995, expose: *„C'est (…) l'objectif choisi avant la mise en oeuvre du traitement qui se trouve à la base de la détermination des opérations à effectuer pour l'atteindre ou espérer l'atteindre et de celle des données soumises à ces opérations. C'est cet objectif qui constitue la finalité. Il ne peut donc être question d'englober dans une finalité un ensemble d'objectifs flous et trop nombreux"* (page 65).

Le considérant (28) de la Directive 95/46/CE souligne *„que les finalités doivent être explicites et légitimes et doivent être déterminées lors de la collecte des données; que les finalités des traitements ultérieurs à la collecte ne peuvent pas être incompatibles avec les finalités telles que spécifiées à l'origine"*.

En outre la finalité doit être légitime. Il appartiendra à la Commission nationale pour la protection des données de même qu'au juge d'apprécier le respect de cette obligation, à travers la grille de lecture que constitue le projet de loi.

Selon Alain Pipers, le *critère général consiste à apprécier cette légitimité par rapport aux activités du maître du fichier*[1] *ou de l'organisation dont il fait partie.*

En ce qui concerne la **compatibilité des finalités:**

„(…) elle n'a pour objectif que d'apprécier si les données à caractère personnel d'un traitement peuvent, ou non, faire l'objet d'un autre traitement ou d'une autre utilisation" (Alain Pipers in ibidem, pages 75-77).

Les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement (b). Le principe de la proportionnalité précise que les données doivent être nécessaires, et non seulement utiles, pour qu'un traitement puisse être accompli. En d'autres termes, *„ce principe vise l'évaluation de l'opportunité d'introduire une donnée à caractère personnel dans un traitement par rapport à la finalité de ce traitement"* (Alain Pipers in ibidem, page 83).

Les données doivent être exactes et, si nécessaire, mises à jour (c). Une règle qui semble évidente, alors que l'exactitude des données est non seulement dans l'intérêt du responsable du traitement lequel ne peut arriver à des résultats exacts et tangibles que si son traitement se base sur des données non erronées. Mais cette règle constitue surtout une mesure de protection dans le chef de la personne concernée, alors que l'objet du traitement de ses données est de mener soit à la connaissance de certains de ces caractères, soit à une décision à son sujet. Le corollaire de cette obligation d'exactitude est évidemment que toute mesure raisonnable doit être prise pour que les données à caractère personnel qui s'avèrent inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

---

1 Ce commentaire est antérieur à la Directive 95/46/CE: la notion de „responsable du traitement" a désormais remplacé celle de „maître du fichier".

Les données à caractère personnel ne doivent être conservées sous une forme permettant l'identification des personnes concernées que pendant la durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées (d). Il s'agit du prolongement du principe de la proportionnalité. Conserver des données sous forme nominative plus longtemps que la durée nécessaire à la réalisation des finalités déclarées, constituerait un traitement de données non nécessaires, donc non pertinentes.

La Directive 95/46/CE prévoit dans son article 6, paragraphe 1. sous b), qu'*„un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les Etats membres prévoient des garanties appropriées*". L'article 4 paragraphe (2) dispose qu'un tel traitement sera soumis à autorisation préalable de la Commission nationale pour la protection des données tel qu'il est organisé à l'article 14.

La qualité des données constitue le principe de base en matière de protection des données, de ce fait il y a lieu de prévoir des sanctions en cas de constat d'une violation des règles développées ci-dessus (article 4 paragraphe (3)).

ad Article 5

Conformément aux dispositions de la Directive 95/46/CE (article 7), l'article 5 du projet de loi prévoit différentes conditions, en application desquelles un traitement portant sur des données à caractère personnel est considéré comme légitime.

(1) Les conditions de légitimité sont alternatives.

Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis (a): par exemple les entreprises sont soumises par la loi à la tenue d'une comptabilité, en conséquence elles effectuent des opérations dans lesquelles elles traitent les données à caractère personnel de leurs clients et fournisseurs; les chefs d'entreprises sont obligés de communiquer les données à caractère personnel de leurs employés et ouvriers à la sécurité sociale; etc.

Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données à caractère personnel sont communiquées (b): la majorité des traitements effectués pour compte de l'Etat par les ministères, les administrations, les services publics ou autres établissements publics tombent dans cette „catégorie" de légitimation, mais il peut également s'agir de traitements qui sont effectués par les administrations communales ou par des personnes soumises au droit privé, telles que les chambres professionnelles.

Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie (c) (ouverture d'un compte en banque, achat d'une voiture automobile, fourniture en eau, gaz, électricité, …) **ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci** (demande adressée à une compagnie d'assurance en vue de l'obtention d'une police assurance-vie, …).

Le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données à caractère personnel sont communiquées, à condition que ne prévalent pas l'intérêt ou les libertés et droits fondamentaux de la personne concernée (d). Il incombera à la Commission nationale pour la protection des données à laquelle les traitements à mettre en oeuvre sont notifiés, de contrôler si la balance d'intérêts introduite par cette condition de légitimité a été correctement évaluée par celui qui entend mettre en oeuvre le traitement. A savoir, si l'intérêt légitime, normalement économique ou commercial, poursuivi par celui qui traite les données à caractère personnel ou auquel ces données seront communiquées, ne porte pas atteinte à la vie privée des personnes concernées.

Exemples illustrant le respect d'une balance d'intérêts:

– les données à caractère personnel sont traitées de manière professionnelle exclusivement en vue d'une publication dans la partie rédactionnelle d'un média à caractère périodique;
– les données à caractère personnel sont traitées à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, à condition toutefois que les résultats soient publiés sous une forme ne permettant pas d'identifier les personnes concernées;
– les données à caractère personnel sont traitées dans le but d'évaluer le crédit d'une personne, à condition toutefois qu'elles ne soient ni sensibles ni constitutives de profils de la personnalité et qu'elles ne soient communiquées à des tiers que si ceux-ci en ont besoin pour conclure ou exécuter

un contrat avec la personne concernée. Toutefois, dès lors que la conclusion du contrat entre la personne concernée et le responsable du traitement, ou encore le tiers auquel les données ont été communiquées dépend de leur contenu (la personne a-t-elle un crédit suffisant pour bénéficier de tel droit ou contrat, est-elle suffisamment crédible pour bénéficier de telles conditions dans son contrat de prêt, d'assurance automobile …), la procédure à suivre sera celle de l'autorisation préalable (cf. article 14).

Le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée (e) n'exige pas de commentaire particulier.

La personne concernée doit donner son consentement exprès (f). Il est de doctrine généralement établie, qu'un consentement qui est donné librement peut à tout moment être retiré par la personne concernée. Toutefois le retrait du consentement ne pourra pas avoir d'effet rétroactif sur le traitement des données à caractère personnel effectué licitement au cours de la période précédant le retrait du consentement.

ad Article 6

Le projet de loi reprend de la Directive 95/46/CE le **principe de l'interdiction du traitement de catégories particulières de données à caractère personnel dites „données sensibles"** (article 8 de la Directive). Il s'agit des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé et à la vie sexuelle. On y a ajouté les données génétiques. Cet ajout est opportun alors que le traitement de données génétiques est de plus en plus fréquent tant dans le domaine de la santé que dans celui des assurances et de l'emploi. De plus, la définition de donnée à caractère personnel (article 2, point (a) du projet de loi) fait référence à l'identité génétique de la personne concernée.

La définition de la „ donnée génétique" (art. 6 (1) (b)) en question est reprise de la Recommandation No R (97) 5 du 13 février 1997 du comité des ministres du Conseil de l'Europe relative à la protection des données médicales. La définition précise, que la donnée génétique *„se réfère également à toute donnée portant sur l'échange de toute information génétique (gènes) concernant un individu ou une lignée génétique, en rapport avec les aspects, quels qu'ils soient, de la santé ou d'une maladie, qu'elle constitue ou non un caractère identifiable"*, la lignée génétique étant considérée comme la lignée *„constituée par des similitudes génétiques résultant d'une procréation et partagées par deux ou plusieurs individus"*.

Contrairement à la loi du 31 mars 1979 qui ne prévoyait pas d'exceptions au principe de l'interdiction du traitement de données à caractère personnel sensibles, la Directive 95/46/CE fixe, de manière détaillée, les règles matérielles légitimant le traitement de telles données. Les exceptions à l'interdiction du traitement de données sensibles (art. 6 paragraphe (2)) ne dispensent pas de l'obligation de prévoir en droit interne des garanties appropriées, telles qu'exigées par la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe (Convention 108), notamment des mesures techniques et organisationnelles appropriées lors du traitement de ces données, afin que seules les personnes autorisées aient accès aux données en question.

Ainsi en matière de données génétiques, le traitement se fait souvent sans dissociation entre la donnée et son support organique. La mention de l'indisponibilité du corps humain appréhende et prohibe les comportements déviants tels l'eugénisme ou la reproduction cellulaire aboutissant au clonage. Cette disposition permet également de réserver l'avenir et d'inclure des hypothèses scientifiques non encore connues.

L'article 6 paragraphe (2) (a) prévoit que l'interdiction énoncée au paragraphe (1) ne s'applique pas lorsque la personne concernée a donné son consentement exprès au traitement de ses „données sensibles" sauf si elle est dans l'incapacité de le faire. Le projet vise ici l'indisponibilité du corps humain et sauf si une loi prévoit expressément que le principe de l'interdiction ne peut être levé par le consentement de la personne concernée ceci dans le but de protéger les droits et le cas échéant la vie de la personne concernée.

Il existe même des cas où il est nécessaire et légitime de traiter des données à caractère personnel dites sensibles, tel que dans les domaines du travail, de la circulation routière, des assurances, de la statistique et de la recherche, comme dans ceux de la justice et de la police, domaines dans lesquels il n'est pas toujours possible, ni par ailleurs opportun, de requérir le consentement de la personne concernée, voire de toutes les personnes concernées par le traitement.

Ainsi les exceptions aux interdictions sont-elles prévues comme suit:

(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 une disposition légale.

(c) Le traitement 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 qui inclut l'incapacité psychique ou dans l'incapacité juridique de donner son consentement (ex. traitement dans un cas d'urgence médicale, la personne concernée se trouve dans le coma et il y a lieu de procéder à une greffe d'organe).

(d) Le traitement est effectué avec le consentement exprès de la personne concernée, dans le cadre des activités d'une fondation, d'une association ou de tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux données nécessaires et relatives aux 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 exprès des personnes concernées. Le considérant (33) de la Directive 95/46/CE mentionne à ce sujet les *„activités légitimes* [de] *certaines associations ou fondations dont l'objet est de permettre l'exercice de libertés fondamentales*" (associations religieuses, partis politiques, syndicats, …). Encore faut-il dans ce cas que des garanties appropriées, notamment d'ordre technique, évitent des traitements abusifs.

(e) Le traitement porte sur des données à caractère personnel manifestement rendues publiques par la personne concernée. Exemple: il serait certainement vain de demander à un homme politique de donner son consentement explicite pour que l'on puisse „révéler" qu'il appartient à tel ou tel parti politique.

(f) Le traitement mis en oeuvre conformément aux règles de procédures judiciaires est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice dès lors qu'il est effectué à cette fin exclusive. Exemple: une analyse du sperme, respectivement du sang, peut s'avérer nécessaire pour déterminer, en cas de doute, l'auteur d'un viol ou encore pour rétablissement d'un lien de filiation.

L'article 6 paragraphe (2) (g) reprend l'idée du considérant (34) de la Directive 95/46/CE qui énonce que *„les Etats membres doivent également être autorisés à déroger à l'interdiction de traiter des catégories de données sensibles lorsqu'un motif d'intérêt public important le justifie dans des domaines tels que la santé publique et la protection sociale – particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie – et tels que la recherche scientifique et les statistiques publiques; qu'il leur incombe, toutefois, de prévoir les garanties appropriées et spécifiques aux fins de protéger les droits fondamentaux et la vie privée des personnes";* tout en le soumettant à autorisation telle que prévue à l'article 14. Le reste du contenu de ce considérant est repris à l'article 7.

L'article 6 (2) (h) vise le traitement soumis à l'autorisation par voie réglementaire (article 17). Il s'agit des traitements nécessaires à la prévention, à la recherche, à la constatation et à la poursuite des infractions pénales réservés, conformément à leurs missions légales et réglementaires respectives, aux organes de la police grand-ducale, de l'Inspection générale de police et de l'administration des douanes et accises. On vise donc ici les matières relevant de la police judiciaire, de la défense, de la sécurité publique et de la sûreté de l'Etat.

L'article 6 paragraphe (3) vise les procédures judiciaires et l'enquête pénale soumises aux règles de la procédure pénale. La loi ne saurait réglementer ou exclure de façon générale ces matières. Toutefois, elle prévoit une limitation relative aux données génétiques dans la mesure où celles-ci ne peuvent être traitées que dans le cadre de l'administration de la preuve pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée. Ces limites sont reprises de la recommandation R97/5 du Conseil de l'Europe.

L'article 6 paragraphe (4) traite des données génétiques pour les soumettre à un régime particulier. Ce régime est plus restrictif que celui des catégories particulières de données, dites données sensibles visées au paragraphe (1) dans la mesure où le traitement de données génétiques n'est possible que dans certains cas bien précis à savoir:

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

– le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice dès lors qu'il est effectué à cette fin exclusive.

Le traitement de données génétiques est encore possible:

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

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

Les dispositions des articles 7 (Traitement de catégories particulières de données par les services de la santé), 8 (Traitement de données judiciaires) et 9 (Traitement réalisé dans le cadre de la liberté d'expression) complètent et spécifient les dispositions de l'article 6.

ad Article 7

L'article 7 paragraphe (1) relatif à la licéité du traitement de catégories particulières de données, dites données sensibles reprend l'article 8 paragraphe (3) de la Directive.

Lorsque le traitement de catégories particulières de données, est nécessaire aux fins de la médecine préventive, des diagnostics médicaux et de l'administration de soins ou de traitements médicaux, la licéité du traitement est garantie, *„lorsque le traitement de ces données est mis en oeuvre (…) par des personnes soumises à une obligation de secret professionnel"* (considérant (33) de la Directive 95/46/CE), celui-ci sera possible.

C'est la relation de confiance „patient-médecin", assortie de la liberté dont dispose le patient de choisir son médecin, qui confère à ce dernier ainsi qu'aux personnes qui l'entourent dans l'exercice de sa profession, le droit de traiter de façon licite les données relatives à la santé de ses patients.

Par ailleurs, le traitement de telles catégories de données est licite, s'il est nécessaire à la gestion de services de santé, de la recherche scientifique dans le domaine de la biologie et de la médecine. Il pourra être mis en oeuvre par les organismes de sécurité sociale et les administrations et services publics qui traitent ces données en exécution de leurs missions légales et réglementaires et là encore si le responsable du traitement est soumis au secret professionnel.

L'article 7 paragraphe (2) prévoit que les traitements seront soumis à la procédure de l'autorisation préalable de l'article 14.

Toutefois l'article 7 paragraphe (3) prévoit pour des raisons pratiques la procédure sera celle de la notification – lorsqu'un traitement est mis en oeuvre conformément à l'article 36 de la loi du 28 août 1998 sur les établissements hospitaliers, ou lorsqu'il s'agit de la relation „médecin-patient" afin de permettre le bon fonctionnement des services de santé.

L'article 7 paragraphe (4) prévoit qu'un règlement grand-ducal établira les modalités d'après lesquelles les données visées à l'article 6 paragraphe (1) peuvent être communiquées à un tiers, ou peuvent être utilisées à des fins de recherche.

ad Article 8

L'article 8 paragraphes (1), (2) et (3), reprend les dispositions de l'article 8 paragraphe (5) de la Directive.

Il faut souligner qu'aucun traitement de données judiciaires n'est „réservé" à l'Etat, mais que les traitements de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peuvent être effectués qu'en exécution d'une disposition légale. Cette disposition intègre, bien évidemment, les données relatives à la protection de la jeunesse.

Toutefois, le recueil exhaustif des condamnations pénales (casier judiciaire) continue à être tenu sous le contrôle de l'autorité publique compétente de même que les données relatives aux jugements civils ou administratifs, ainsi qu'aux sanctions administratives.

ad Article 9

L'article 9 de la Directive 95/46/CE prévoit qu'il y a lieu de concilier, si nécessaire, le droit à la vie privée avec les règles régissant la liberté d'expression pour les traitements effectués à des fins de journalisme ou d'expression artistique ou littéraire.

Il incombera au juge de vérifier que la finalité poursuivie, à savoir le journalisme ou l'expression artistique ou littéraire, a été respectée, et que la balance des intérêts entre le respect de la vie privée et la nécessaire liberté d'expression aura été prise en considération.

Les traitements effectués à des fins de journalisme ou d'expression artistique ou littéraire pourront être mis en oeuvre par dérogation aux prohibitions et restrictions générales prévues par le projet de loi ou encore dans des conditions dérogatoires au droit commun.

1) Les dérogations aux prohibitions et restrictions à l'article 9 reprennent celles de la Directive 95/46/CE:

– les traitements mis en oeuvre à des fins de journalisme ou d'expression artistique ou littéraire sont possibles par dérogation à la prohibition de l'article 18 paragraphe (1) et peuvent donc faire l'objet de flux transfrontaliers, y compris à destination de pays n'assurant pas un niveau de protection adéquat. Dans ce cas de figure la liberté d'expression prime sur la protection des données personnelles.
– les traitements mis en oeuvre à des fins de journalisme ou d'expression artistique ou littéraire sont possibles par dérogation à la prohibition de l'article 6 paragraphe (1) et aux restrictions de l'article 8 qui traite des traitements de données relatifs aux infractions, condamnations et mesures de sûreté. Les traitements à des fins de journalisme ou d'expression artistique ou littéraire doivent pouvoir utiliser de telles informations à trois conditions alternatives:
  • Ces données ont été rendues manifestement publiques par la personne concernée. Peu importe le mode de diffusion des informations en question, seule la manifestation de volonté claire et non équivoque de la personne concernée de divulguer les informations importe (exemple: les convictions politiques d'un dirigeant de parti politique sont des données rendues manifestement publiques par la personne concernée).
  • Les données sont en relation étroite avec le caractère public de la personne concernée. Tout personnage public véhicule certaines données qui, même si elles ressortent de la sphère de sa vie privée, ne peuvent être protégées car elles sont en relation étroite avec le caractère public de sa personne.
  • Les données sont en relation étroite avec le caractère public du fait dans lequel la personne concernée est impliquée. On peut citer l'exemple de l'incendie d'un établissement psychiatrique, fait divers relayé par les médias qui, sur place, entendent les victimes et recueillent leur témoignage. Il est clair que les victimes sont aussi des patients de cet établissement. Or, l'événement étant public, les données relatives aux personnes impliquées d'une manière ou d'une autre dans cet événement sont publiques.

2) Le traitement mis en oeuvre dans des conditions dérogatoires au droit commun

– Le journaliste doit disposer d'une certaine marge de manoeuvre et l'obligation d'informer la personne concernée ne lui est pas applicable dans la mesure où elle compromettrait la collecte des données. Il est clair que le journaliste doit pouvoir agir en toute liberté et traiter des données sans qu'il ne soit contraint de dévoiler, y compris à la personne concernée, le thème de son article et sa façon de le traiter.

  Exemple: le journaliste verrait sa collecte de données compromise s'il informait la personne concernée de son intention de rédiger un article destiné à démontrer, par exemple, que le taux d'analphabétisme est supérieur dans certains quartiers de la cité par rapport à d'autres. La personne pourrait refuser de répondre à certaines questions ou être incitée à donner des réponses inexactes afin de mettre le journaliste sur une mauvaise piste ce qui compromettrait ainsi la collecte.
– Lorsque la collecte n'est pas effectuée auprès de la personne concernée elle-même, l'information de la personne concernée n'est pas obligatoire si cela:

- compromet la collecte (exemple: le journaliste n'a pas à informer les personnes concernées s'il décide de recenser toutes les personnes étrangères qui disposent d'une résidence secondaire, l'ampleur du travail d'information pouvant compromettre la collecte des données);
- compromet le projet de publication (exemple: le journaliste souhaite faire éclater un scandale en choisissant le moment le plus opportun pour la publication de son article; s'il révèle ses intentions en informant préalablement les personnes concernées, il est clair que l'effet „éclat" recherché est manqué);
- compromet la mise à disposition du public, de quelque manière que ce soit des données traitées à des fins de journalisme ou d'expression artistique ou littéraire;
- fournirait des indications permettant d'identifier ses sources d'informations

– Afin de ne pas mettre en danger la liberté d'expression, la notification obligatoire auprès de la Commission d'un traitement effectué à des fins de journalisme ou d'expression artistique ou littéraire, ne renseigne que sur les nom(s) et adresse(s) du responsable du traitement ou de son représentant.
– Lorsque, de manière générale, il y a investigation de la Commission, celle-ci, dans le respect des règles relatives à la liberté d'expression, ne peut opérer qu'en présence du président de l'organe représentatif de la presse. Il appartient à la loi sur la presse en cours d'élaboration de préciser quel est cet organe représentatif. Ce dernier est le garant du respect des obligations relevant du statut professionnel du journaliste (article 9 paragraphe (3)).

Une balance des intérêts entre les droits de la personne concernée et les droits du journaliste ou de l'artiste doit être respectée de sorte que la personne concernée doit pouvoir exercer son droit d'accès et de rectification à ses données traitées à des fins de journalisme. Toutefois, le projet de loi prévoit que dans ce cas la personne concernée ne dispose que d'un droit d'accès indirect prévu à l'article 28 paragraphe (4). Aux fins de cet article, tant que les données auxquelles l'accès est demandé n'ont pas été publiées, leur communication ou toute information disponible sur leur origine ne peut se faire qu'indirectement par le biais de la Commission.

En cas de difficulté rencontrée dans la conciliation entre les droits de la personne concernée et le respect nécessaire des obligations professionnelles et déontologiques du journaliste, la Commission et l'organe représentatif de la presse se concertent afin de trouver une solution équilibrée conformément à l'article 29. Le droit d'accès indirect, ne pourra donc être différé ou limité que sous le contrôle de la Commission (dans les conditions de l'article 9 paragraphe (3)).

La structure du droit d'accès au regard de la liberté d'expression est donc la suivante:

1. le droit d'accès est reconnu à la personne concernée (principe énoncé à l'article 28 paragraphe (4));
2. l'article 28 paragraphe (4) définit les conditions d'exercice du droit d'accès indirect de la personne concernée. Celui-ci est une limitation au droit d'accès qui est à l'article 9 de la Directive;
3. l'article 29 qualifie clairement la situation des journalistes comme faisant partie des hypothèses permettant de limiter ou de différer le droit d'accès, ceci rappelle qu'hormis les règles particulières définies à l'article 28 paragraphe (4), celles définies à l'article 29 sont d'application à cette hypothèse.

ad Articles 10 et 11

Le projet de loi inclut les traitements de données à des fins de surveillance comme par exemple la vidéosurveillance ainsi que toute autre forme de surveillance électronique. Elle distingue entre le traitement de données à des fins de surveillance sur le lieu de travail (article 11) et d'autres hypothèses (article 10: régime général). Les traitements de données à des fins de surveillance sont assortis de conditions et de procédures assez strictes par souci de protection des personnes surveillées et afin d'éviter un phénomène de „big brother is watching you".

Les traitements de données à des fins de surveillance entrent dans le champ d'application de la Directive hormis ceux mis en oeuvre et nécessaires à la prévention, la recherche, la constatation et la poursuite d'infractions pénales soit les activités de l'Etat dans les domaines du droit pénal.

Les traitements à des fins de surveillance visant toutes formes de surveillance dont notamment la vidéosurveillance font partie intégrante du champ d'application de la Directive 95/46/CE (considérant 16) et sont soumis au régime général de celle-ci. Le projet de loi ne fait qu'y renvoyer tout en précisant certaines règles lorsque cela s'avère nécessaire pour la protection des droits des personnes concernées.

Les traitements relatifs à la prévention, la constatation et la poursuite d'infractions pénales ainsi qu'aux activités de l'Etat dans les domaines du droit pénal[1] ont été volontairement inclus dans le champ d'application du projet de loi (cf. supra ad Art. 3). Dès lors ils sont également soumis aux règles matérielles de la loi tout en connaissant un régime dérogatoire et spécial s'agissant de la procédure de mise en oeuvre (cf. article 17).

ad Article 10

L'article 10 traite de toutes les formes de surveillance et en particulier de la vidéosurveillance et des nouvelles technologies. L'axe principal de cet article est la finalité du traitement.

L'article 10 n'instaure pas de régime particulier mais précise certaines dispositions particulières dans un environnement particulier. En essayant d'éviter d'une part la distinction entre domaine public et domaine privé et d'autre part, que l'on puisse installer à l'avenir des caméras partout, le présent article définit les cas où la loi autorise le traitement à des fins de surveillance (paragraphe 1) (ex. gares, aérogares, moyens de transports publics, lieux accessibles au public tels que les banques, les écoles etc.) et définit les conditions dans lesquelles celui-ci peut-être mis en oeuvre (paragraphes 2 à 4). Il s'efforce de trouver un équilibre entre l'Etat de droit (cf. surveillance dans le cadre de l'article 17) et le respect de la vie privée de chacun. Le projet de recommandation *sur la protection des données à caractère personnel collectées et traitées à des fins de surveillance (Conseil de l'Europe, mai 99; réf CJ-PD-GTNT (98)4rev2)* a servi de base à la rédaction du présent article.

Le paragraphe 1 (b) traite de la surveillance et de l'Etat dans son rôle de garant de la sécurité publique. Il limite le champ de la surveillance à ce qui est nécessaire à la prévention, la recherche, la constatation et à la poursuite d'infractions pénales. Ce sont les hypothèses de l'article 17 paragraphe (1) qui sont reprises, écartant celles de l'article 17 paragraphe (2).

En outre l'article 10 paragraphe 1 (c) permet de limiter le risque d'abus de droit en matière de droit de propriété. Il semble légitime qu'une personne rendant visite à une autre dans sa résidence soit informée de l'existence d'une caméra braquée sur elle ou de tout autre mode de traitement de données, dès lors que le traitement de données ne se ferait pas dans le cadre d'activités exclusivement personnelles ou domestiques (article 3 paragraphe (3) de la loi)[2].

L'article 10 paragraphes (2) et (4) rappelle et précise l'obligation d'information notamment de l'article 26 tout en précisant certains aspects spécifiques à la surveillance. Il est fait référence au recommandé par voie électronique reconnu dorénavant au même titre que le recommandé par voie postale.

ad Article 11

L'article 11 prévoit la surveillance sur le lieu de travail. Il s'inspire de la convention collective de travail belge numéro 68 qui transpose, dans le secteur du droit du travail, les dispositions de droit commun de la Directive 95/46/CE tout en les précisant. L'article 11 permet à l'employeur de surveiller sous certaines conditions ses employés sur le lieu de travail. Le présent article tient compte de certaines pratiques mises en oeuvre sur le lieu de travail tout en apportant des garanties nécessaires aux droits des travailleurs. C'est la raison pour laquelle la surveillance sur le lieu de travail est soumise à des conditions assez strictes. Ainsi la surveillance du travailleur afin de déterminer sa rémunération n'est-elle permise que de façon temporaire et après que l'employeur ait informé le Comité mixte, à défaut la délégation du personnel ou à défaut encore l'Inspection du Travail et des Mines qui devront être informés de la durée de la collecte des données. Il y a lieu de préciser que cette information se fait sans préjudice des autres dispositions du projet de loi et notamment celles relatives à l'information, au droit d'accès et au droit de rectification de la personne concernée. Notons, qu'à la lumière des articles 6 et 7 relatifs aux catégories particulières de données et hormis le consentement exprès de la personne concernée, l'employeur ne pourra pas traiter de ce type de données, dans le cadre de la surveillance de son entreprise. On renvoie ici pour lecture sur ce point, à l'exposé des motifs qui complète ces développements.

---

1 La prévention, la recherche, la constatation et la poursuite d'infractions pénales soit les activités de l'Etat dans les domaines du droit pénal.

2 Rappelons que l'activité domestique d'une personne physique n'entre pas dans le champ d'application du projet de loi et qu'un traitement de données mis en oeuvre dans ce cadre est totalement libre.

Chapitre III. *Notification et publicité des traitements*

ad Article 12

L'article 12 du projet de loi reprend en substance les dispositions de l'article 18 de la Directive. L'article 12 paragraphe (1) a pour objectif *„d'organiser la publicité des finalités et des principales caractéristiques. du traitement en vue de son contrôle* (considérant (48) de la Directive 95/46/CE)" par le biais de la notification.

Si le traitement est conforme aux conditions de légitimité prévues par la loi, il peut être mis en oeuvre immédiatement, la Commission se réservant le droit, a posteriori, d'ordonner l'interruption de la collecte des données ou du traitement, ainsi que la destruction des données s'il s'avérait que le traitement notifié n'est pas conforme aux dispositions de la présente loi.

Cependant l'article 12 paragraphe (2) prévoit des dérogations à l'obligation de notification dans quatre cas:

- lorsqu'un chargé de la protection des données a été nommé; dans ce cas, c'est à ce dernier d'apprécier la situation et de faire respecter les dispositions de la loi;
- lorsque le traitement a pour seul objet la tenue d'un registre public;
- lorsque le traitement est effectué dans le cadre de l'article 17 dont les règlements grand-ducaux sont sujets à publication au Mémorial;
- lorsque le traitement est effectué dans le cadre de l'article 6 paragraphe 2 (f) dont le principe du contradictoire et les règles de procédures judiciaires applicables constituent une protection suffisante à la personne concernée.

Même si la tenue du registre quant à sa forme n'est pas sujet à notification, ceci ne veut pas dire que les données qui forment le contenu ne doivent pas suivre la procédure de notification.

Toute absence de notification ou toute fourniture, lors de la notification, d'informations sciemment inexactes entraînent l'application de sanctions pénales (article 12 paragraphes (3) et (4)).

ad Article 13

Cet article détermine les informations que la notification d'un traitement doit comprendre (article 19 de la Directive in extenso). A ces informations prévues par la Directive, le projet de loi ajoute celle relative à la durée de conservation des données. La durée est une précision nécessaire à la définition des besoins du traitement en cause. Cette exigence va dans le sens du principe de la finalité de la directive.

Il y a lieu de mentionner l'information relative au pays de destination qui constitue une information essentielle dans l'optique de la libre circulation des données. Il faudra apprécier si le pays destinataire assure un niveau de protection „adéquat" pour savoir si la sécurité des données transférées à l'étranger est assurée.

Tout changement affectant les informations requises sont à notifier à la Commission préalablement à leur mise en oeuvre (paragraphe 2). La notification se fait auprès de la Commission, soit sur support papier, soit sur disquette, suivant un schéma établi par l'autorité (paragraphe 3). Il est accusé réception de la notification.

Si la notification, conformément au considérant (48) de la Directive 95/46/CE a *„pour objet d'organiser la publicité des .finalités du traitement, ainsi que de ses principales caractéristiques, en vue du contrôle au regard des dispositions nationales"* en matière de protection des données, cela vaut aussi bien par rapport à la Commission que par rapport au grand public, c'est-à-dire, des personnes concernées.

Quiconque contrevient aux dispositions de la notification est passible d'une sanction pénale (paragraphe 4).

Un règlement grand-ducal fixera le montant et les modalités de paiement de la redevance proportionnellement au coût du service presté pour chaque notification (paragraphe 5).

Dans le cadre des nécessités liées à la sûreté de l'Etat, la défense et à la sécurité publique, les administrations et le responsable du traitement, lors de la notification et de l'information de la personne concernée (article 26) pourront prévoir que les autorités publiques chargées de ces missions seront les destinataires des données traitées.

ad Article 14

L'article 20 de la Directive prévoit un contrôle préalable pour la mise en place de traitements de données susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées.

L'article 14 du projet de loi met en place un tel système qui prend la forme d'une autorisation préalable accordée par la Commission. Certains traitements présentent a priori des risques particuliers au regard des droits et libertés des personnes concernées pour différentes raisons (paragraphe (1)).

La première raison est en relation avec la nature des données traitées. Un traitement portant sur une des catégories particulières de données visées à l'article 6 paragraphe (1) présente un risque particulier. Ces données touchent en effet directement à la vie privée. On ne peut envisager la mise en oeuvre d'un traitement relatif aux opinions politiques d'une catégorie de personnes identifiées, sans que soit nécessaire une autorisation préalable basée sur un contrôle a priori strict des dispositions de la loi. Toutefois dans deux hypothèses on déroge à cette exigence d'autorisation. La première est l'hypothèse de la sauvegarde de la vie et la seconde est celle du fonctionnement des associations et autres fondations.

La deuxième raison est en relation avec la finalité du traitement. La finalité est un des fondements de la protection de la personne concernée par le traitement. Cette protection peut être renforcée par le système de l'autorisation préalable.

Dès lors que la finalité originaire est manifestement dépassée ou changée, l'autorisation préalable est requise (traitement de données à des fins historiques, statistiques ou scientifiques alors que la collecte à l'origine était faite à une toute autre fin; l'interconnexion en ce qu'elle peut-être faite entre deux sources de données structurées ou non ayant une finalité différente). A propos de l'interconnexion et conformément à la politique générale de la Commission européenne, la Commission nationale pour la protection des données vérifiera tout particulièrement la compatibilité des finalités des traitements à interconnecter.

Enfin, la finalité d'un traitement, même en restant identique du début à la fin peut tout de même exiger une autorisation préalable. A ce propos, le considérant 53 de la Directive vise clairement certains traitements comme présentant *„des risques particuliers au regard des droits et libertés des personnes concernées, du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat …*". Ici, sont particulièrement visés les traitements concernant spécialement le crédit et la solvabilité, quelle que soit la profession en cause (banque, assurances ou autres professionnels du secteur financier). En effet et le plus souvent, de tels traitements conditionnent l'accès au contrat. Ils devront donc être soumis à autorisation préalable.

L'article 14 paragraphe (2) établit la procédure à suivre en matière d'autorisation préalable.

ad Article 15

Cet article transpose l'article 21 de la Directive.

La Commission tient un registre des traitements qui lui sont notifiés. Ce registre prend la relève du répertoire national des banques de données organisé par l'article 13 de la loi du 31 mars 1979 et renseigne à propos des informations notifiées sur chaque traitement. Pour les traitements soumis à autorisation préalable, le registre renseigne en plus sur l'autorisation émise par la Commission. Sont exclus de l'obligation de publicité, par application combinée de l'article 12 paragraphe (2) (c) et de l'article 15 paragraphe (1), les traitements soumis à autorisation préalable par voie réglementaire en vertu de l'article 17.

Toutes les informations du registre sont (gratuitement) accessibles au public, à l'exception toutefois de l'information relative aux mesures prises pour assurer la sécurité du traitement. Cette restriction semble utile et nécessaire afin de ne pas mettre en péril ces mesures.

ad Article 16

L'interconnexion constitue par définition un traitement de données à caractère personnel.

La législation de 1979 excluait toute interconnexion. Cette prohibition n'est plus adaptée aux besoins actuels ni aux technologies disponibles que ce soit dans le secteur privé ou dans le secteur public. Par exemple, la sécurité sociale a besoin d'un cadre juridique clarifié pour la gestion de ses missions afin d'accéder à certains traitements d'autres organismes publics (établissements hospitaliers, caisses …). Il est donc nécessaire de permettre de telles interconnexions.

Toutefois, le considérant 53 de la Directive souligne qu'il est nécessaire de soumettre à autorisation préalable „certains traitements susceptibles de présenter des risques particuliers au regard (…) de leurs finalités (…) ou du fait de l'usage particulier d'une technologie nouvelle.

L'interconnexion de traitements qui sont normalement à finalités différentes, présentent des dangers évidents pour le respect de la vie privée des personnes. En effet, le respect du principe de la finalité[1] ainsi que l'usage particulier d'une technologie nouvelle qui sera la règle sont deux indices qui appellent à une vigilance toute particulière.

Ainsi, l'article 16 soumet tout projet d'interconnexion entre deux ou plusieurs traitements, que leurs responsables relèvent du secteur public ou du secteur privé, à l'autorisation préalable de la Commission. La Commission examinera notamment la licéité du traitement et les garanties concernant la compatibilité des finalités des traitements à interconnecter. Ce système a vocation à ne pas freiner le processus de l'interconnexion et a pour but de garantir un niveau de protection accru.

Les modalités de mise en oeuvre de l'interconnexion peuvent être précisées par règlement grand-ducal. Ce règlement grand-ducal doit toujours être conforme à l'esprit de la loi et de la directive et respecter les missions de la Commission tout en restant une mesure d'exception.

ad Article 17

Le paragraphe (1) soumet la création d'un traitement dans le cadre des missions de police judiciaire à une procédure de contrôle préalable spécifique. Cette création se fait par voie de règlement grand-ducal et fait intervenir pour avis la Commission. Ainsi, l'article 17, paragraphe (1) de la présente loi reprend en fait la teneur du paragraphe (1) de l'article 12-1 de la loi du 31 mars 1979, telle que modifiée par celle du 30 septembre 1992. Il ajoute aux autorités publiques compétentes à côté des organes du corps de la police grand-ducale, ceux de l'administration des douanes et accises qui s'est vue confié par le législateur national, de nouvelles tâches en matière de prévention, de recherche, de constatation et de poursuite des infractions.

La procédure prévue au paragraphe (1) se résume comme suit: le règlement grand-ducal autorise et les autorités policières visées par la loi traitent les données sous la responsabilité du Procureur d'Etat territorialement compétent.

Le paragraphe (2) dispose que les traitements nécessaires à la sauvegarde de la sûreté de l'Etat et de la défense, de même que d'autres traitements en relation avec la sécurité publique sont autorisés selon la procédure ci-dessus.

Chapitre IV. *Transfert de données vers des pays tiers*

ad Article 18

Pour transférer des données vers un pays tiers celui-ci doit garantir un niveau de protection adéquat (article 25 de la Directive).

Il incombe au responsable du traitement d'apprécier (paragraphe (2)) le caractère adéquat du niveau de protection du (des) pays à destination du(des)quel(s) il envisage de transférer des données à caractère personnel.

Le paragraphe (3) oblige le responsable du traitement à informer la Commission nationale pour la protection des données, dès qu'il a un doute quant au niveau adéquat de protection des données. Cette disposition s'apparente à l'obligation de déclaration de soupçon des banques et autres professionnels du secteur financier dans la lutte contre le blanchiment. Elle constitue une obligation de coopération renforcée à charge du responsable du traitement.

Si, d'après l'article 31 de la Directive 95/46/CE, le niveau de protection d'un pays tiers a été reconnu comme adéquat, un transfert de données vers ce pays peut avoir lieu sans autre restriction. Par contre, si la Commission européenne ou la Commission nationale pour la protection des données devrait constater qu'un pays tiers n'offre pas un niveau de protection adéquat, il sera interdit à tout responsable du traitement d'„exporter" des données vers ce pays.

---

1 Le principe de finalité exige pour un traitement qu'une ou plusieurs finalités soient toujours prédéfinies.

ad Article 19

Les dérogations prévues par l'article 19 paragraphe (1) (article 26 de la Directive) permettent d'effectuer des transferts de données vers des pays tiers n'assurant pas un niveau de protection adéquat sous certaines conditions qui viennent en quelque sorte „combler" le manque de protection adéquate.

Ainsi, la première des dérogations est le consentement exprès de la personne concernée (a). La Directive et la loi font donc peser la responsabilité sur la personne concernée elle-même, cette dernière n'est plus protégée malgré elle, mais elle doit faire face à ses responsabilités et autoriser ou non le transfert de données la concernant. Cependant, pour que la personne concernée puisse exercer de façon effective son droit de consentir ou non au transfert envisagé par le responsable du traitement, encore faut-il qu'elle soit informée de façon non équivoque et de manière exhaustive par le responsable du traitement. On peut d'ores et déjà remarquer que via Internet, cette information claire, précise et complète ne sera peut-être pas toujours présente. Le consentement de la personne concernée connaîtra différentes déclinaisons dans le cadre de l'exécution d'un contrat auquel elle est partie (b).

De même l'intérêt de la personne concernée à la conclusion d'un contrat, la sauvegarde d'un intérêt public important, les nécessités inhérentes au fait d'ester en justice, la sauvegarde de la vie, sont autant de cas permettant de déroger à la prohibition (c et d).

En outre la Commission peut autoriser, sous différentes conditions, un transfert ou un ensemble de transferts vers un Etat tiers n'assurant pas de protection adéquate. Dans ce cas, le responsable du traitement doit non seulement motiver les raisons à l'origine du transfert envisagé, mais également offrir des garanties suffisantes au regard de la protection de la vie privée des personnes en cause. En tout cas, il doit respecter la décision de la Commission.

ad Article 20

L'information réciproque entre la Commission nationale pour la protection des données et le ministre compétent en la matière est la condition sine qua non d'une bonne application de la loi dans la mesure où les Etats membres doivent eux-mêmes tenir la Commission européenne informée des décisions prises. Il est indispensable que l'information circule entre tous les acteurs, afin de garantir une application homogène de la loi.

Dans les relations avec la Commission européenne, la Commission nationale pour la protection des données apprécie comme expert le niveau de protection tandis que le ministre est le relais avec les institutions européennes en tant que membre du Gouvernement.

Chapitre V. *Confidentialité et sécurité des traitements*

ad Article 21

Cet article précise que toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même qui accède à des données à caractère personnel, ne peut les traiter, sauf en vertu d'obligations légales[1], que sur instruction du responsable du traitement. La confidentialité est ainsi renforcée alors que la manipulation des données se fait sur autorisation du responsable du traitement, ce qui limite au minimum la diffusion des données.

ad Article 22

L'article 27 de la loi du 31 mars 1979 prévoyait qu'un règlement grand-ducal pris sur avis du Conseil d'Etat et de la commission consultative „peut déterminer les mesures générales à caractère technique destinées à assurer la sécurité matérielle des banques de données et des traitements", tout en précisant que „l'effet de protection recherché par ces mesures doit être dans un rapport adéquat avec les dépenses qu'elles occasionnent". Pour une raison ou une autre, ce règlement grand-ducal n'a jamais été pris.

Aussi semble-t-il plus adéquat de prévoir dans le nouveau texte de loi les mesures de sécurité nécessaires *„pour protéger les données à caractère personnel 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"* (article 17, paragraphe (1) de la Directive 95/46/CE).

1 Il peut s'agir, par exemple, des dispositions de la législation en matière de blanchiment d'argent.

Les mesures de sécurité à mettre en oeuvre par le responsable du traitement sont celles prévues notamment par l'article 118 de la Convention d'application de l'Accord de Schengen, mesures qui depuis ont été reprises dans d'autres instruments de l'Union européenne et du Conseil de l'Europe.

Ces mesures devront être adoptées compte tenu des risques d'atteinte à la protection des données, mais adaptées à chaque type de traitements. Ainsi, il y a lieu de distinguer selon le volume des données à traiter, la nature des données, la dangerosité du traitement, etc. Il incombe au responsable du traitement et à la Commission d'apprécier la nécessité de l'une ou de l'autre de ces mesures pour chaque traitement envisagé.

Ces mêmes mesures de sécurité doivent être respectées lorsque le traitement est effectué pour compte du responsable du traitement. Dans ce cas, il incombe à ce dernier de choisir un sous-traitant qui apporte des garanties suffisantes, au regard des mesures relatives à la sécurité technique et l'organisation des traitements à effectuer, de même que de s'assurer du respect de ces mesures. A cette fin, les relations entre le sous-traitant et le responsable du traitement doivent être régies par un contrat écrit.

ad Article 23

L'article 23 est un catalogue de mesures de sécurité particulières. Il précise les objectifs à atteindre compte tenu du risque d'atteinte à la vie privée ainsi que de l'état de l'art et des coûts liés à leur mise en oeuvre. Il reprend pour ce faire l'article 118 de la Convention de Schengen[1].

ad Article 24

Cet article soumet au secret professionnel toute personne qui exerce ses fonctions auprès de la Commission, tout chargé de la protection des données, tout expert mandaté par la Commission qui a connaissance de données à caractère personnel dans le cadre de ses fonctions (l'article 28 paragraphe (7) de la Directive vise les membres et agents des autorités de contrôle) ceci, aussi bien pendant qu'après la cessation de leurs fonctions.

Il s'agit donc d'un champ d'application du secret professionnel étendu, sans distinction entre les intervenants. Cette extension est nécessaire dans un domaine où le quotidien est fait de traitements de données touchant l'identité propre à chaque personne concernée. Cette solution est reprise de la loi sur les télécommunications du 21 mars 1997 (Mémorial A-No 18 du 27 mars 1997 p. 761). Dans le cadre de la loi sur les télécommunications le secret professionnel gravite autour de l'ILT et concerne ses membres ainsi que les experts mandatés.

Dans le cadre de la protection des données et hormis la Commission (agents et membres) le secret professionnel ne doit pas seulement concerner les experts éventuellement mandatés et visés par l'expression „toute autre personne qui … accomplit une mission pour son compte". Il doit être également élargi à l'institution du chargé de la protection des données. En effet, exclure le chargé de la protection des données qui participe pourtant au service de la protection des données rendrait vaine toute tentative de convaincre les responsables de traitements que le régime mis en place est loyal et qu'ils peuvent lui faire confiance.

Si le chargé de la protection n'était pas lié par le secret professionnel, cette institution serait vouée à l'échec alors qu'elle offrirait au responsable du traitement moins de garanties que la Commission. On aurait échoué dans la recherche de l'efficacité, la mise en place de ce chargé de la protection des données ayant pour objectif primaire de faciliter le traitement des données personnelles et d'éviter que la Commission ne devienne une institution hypertrophiée et paralysée.

Ce secret professionnel obligeant le chargé de la protection des données n'est toutefois pas opposable à la Commission. L'inopposabilité est conforme à l'article 458 du code pénal qui autorise une telle dérogation. Elle est également conforme à l'esprit de la Directive 95/46/CE qui définit le chargé de la protection des données comme un mécanisme souple mais complémentaire de protection qui en cas de doute doit consulter l'autorité de la Commission (article 20 paragraphe (2) de la Directive).

De la même façon, les prestataires de certification visés par le secret professionnel dans la loi du 14 août 2000 relative au commerce électronique ne pourront opposer le secret professionnel à la Commission. L'articulation des directives „signature électronique" (Directive 1999/93/CE du PE et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques;

1 Loi d'approbation du 3 juillet 1992; Mémorial A 1992 p. 1574.

JOCE L 13/12 du 19.1.2000) et „protection des données“ (Directive 95/46/CE précitée) est précisée à l'article 8 paragraphe (1) de la directive „signature électronique“ est relatif à la protection des données: *„Les Etats membres veillent à ce que les prestataires de service de certification et les organismes nationaux responsables de l'accréditation ou du contrôle satisfassent aux exigences prévues par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.“*

Les prestataires de certification sont en fait les responsables d'un type de traitement particulier ayant pour finalité l'authentification de la signature ou d'un document électronique. Cette finalité particulière a entraîné la sujétion à un système de secret professionnel.

Parallèlement ces prestataires de certification sont soumis au droit de la protection des données. Ceci est nécessaire dans un cadre libéralisé afin de garantir le respect des droits des personnes concernées par les traitements de données à caractère personnel. Une telle garantie repose en grande partie sur la qualité du contrôle a posteriori de la Commission. Or, l'inopposabilité du secret professionnel des certificateurs de signature est absolument nécessaire pour garantir un tel contrôle de la Commission. Ceci est logique alors que les certificateurs ne sont en fait qu'une catégorie de responsables de traitements soumis à ce titre au droit de la protection des données. Ils doivent donc pouvoir être contrôlés par la Commission s'agissant (uniquement!) de leurs obligations aux termes de la législation sur la protection des données au même titre qu'un autre responsable de traitement.

Ainsi, l'architecture de la Directive et du projet de loi en ce qui concerne la confidentialité est la suivante:

1) le responsable du traitement est lié vis-à-vis des personnes concernées par son engagement initial de communiquer les données qu'à des personnes ou des catégories de personnes prédéfinies (articles 10 c), 11 c), 19 paragraphe (1) d) et e) de la directive; articles 26 paragraphe (1) (c) tirets 1, 26 paragraphe (3) (c) tiret 2, article 13 paragraphe (d) et (e) du projet de loi). Il devra toutefois répondre aux sollicitations faites par une autorité publique agissant conformément dans le cadre de ses missions légales (sauf à lui opposer une obligation de secret professionnel propre tel que le secret bancaire). Outre la responsabilité civile, l'engagement du responsable du traitement est sanctionné pénalement;
2) le sous-traitant ainsi que tous les intervenants et toutes les personnes agissant sous l'autorité du responsable du traitement ne traitent des données que sur instruction de celui-ci (article 21 du projet de loi et 16 de la directive) de sorte que toute communication non autorisée est prohibée sauf en vertu d'obligations légales (par exemple l'obligation de donner suite à une injonction d'une autorité publique agissant conformément dans le cadre de ses missions légales). Cette obligation de confidentialité est sanctionnée pénalement (article 24 du projet de loi) et le sous-traitant pourra être sanctionné s'il agissait sans instruction du responsable du traitement ou sans être soumis à une obligation légale;
3) la Commission, le chargé de la protection des données (ainsi que les éventuels experts mandatés) et les prestataires de certification sont liés vis-à-vis de l'extérieur par le même et unique secret professionnel. Aucune communication non conforme à ce secret professionnel n'est possible.
4) la Commission ne pourra se voir opposée un quelconque secret professionnel de la part d'un responsable de traitement (article 7 du projet de loi), d'un chargé à la protection des données ou d'un prestataire de certification. Toutefois le cadre strict de ses missions et les fins du contrôle sévère du respect de la loi interdisent à la Commission toute communication hors de ce cadre alors qu'elle-même est soumise au secret professionnel.

Ainsi, ce système:

– assure aux autorités publiques qu'elles ne seront pas affaiblies dans leurs capacités d'intervention;
– garantit les droits de la personne concernée en évitant une dissémination des données;
– garantit la sécurité juridique nécessaire aux responsables de traitements dans leurs relations avec la Commission, le chargé de la protection et le prestataire de service de certification. Il s'agit d'un système neutre pour la place financière du Luxembourg.

ad Article 25

L'article 25 traite des sanctions relatives à la violation des articles 21, 22 et 23 et n'appelle pas de commentaire particulier.

Chapitre VI. *Droits de la personne concernée*

Ce chapitre propose une nouvelle rédaction des droits de la personne concernée, prévus par la loi du 31 mars 1979, à savoir le droit à l'information et le droit d'accès, de même que les droits connexes à ce dernier, le droit de rectification et le droit d'effacement. Cette nouvelle rédaction est issue de la Directive 95/46/CE qui prévoit en outre le droit d'opposition.

ad Article 26

Le droit à l'information (article 10 de la Directive) concrétise le principe de la bonne foi ou de la transparence du traitement de données à caractère personnel. En effet, sans la transparence du traitement et les informations complètes, la personne concernée ne sera pas en mesure de faire valoir ses droits et de donner, le cas échéant, son consentement libre et informé. Ce que la directive et la loi appellent droit à l'information est du point de vue du responsable du traitement une obligation vis-à-vis de la personne concernée.

Premier cas de figure: les données sont collectées auprès de la personne elle-même. Dans ce cas (article 26 paragraphe (1)), il est prévu que les informations identifiant, d'une part le responsable du traitement et le cas échéant son représentant, d'autre part le traitement et les droits dont bénéficie la personne concernée, doivent être fournies à celle-ci au plus tard au moment de la collecte des données, à moins que la personne concernée ait déjà été informée. L'article 26 paragraphe (2) précise, à l'instar de l'article 18 de la loi du 31 mars 1979, que lorsque la collecte des données se fait moyennant formulaire ou questionnaire, ceux-ci doivent comporter les informations énoncées au paragraphe (1).

Deuxième cas de figure: les données ne sont pas ou n'ont pas été collectées auprès de la personne elle-même, mais proviennent d'un traitement déjà existant. Dans ce cas, l'article 26 paragraphe (3) dispose que le responsable du traitement ou son représentant doit fournir à la personne concernée les informations requises 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.

ad Article 27

L'article 27 (cf. articles 9 et 13 (1) de la Directive) dispose sous quelles conditions et dans quelles circonstances des exceptions au droit à l'information sont autorisées et ceci dans les domaines de la sécurité publique, de la sûreté de l'Etat, de la défense, de même que lors du traitement de données effectué dans le cadre de la protection de la personne (données relatives à la santé en cas d'urgence par exemple), ou de la protection des droits et libertés d'autrui. Les exigences de la liberté d'expression y trouvent une application (article 27 paragraphe (2)) et l'obligation d'information y relative est réduite conformément à l'article 9 du projet de loi (article 9 de la Directive). L'exception la plus importante est celle visée à l'article 27 paragraphe (3); il s'agit des cas où l'information de la personne concernée impliquerait un effort disproportionné (ex. traitement ayant une finalité statistique, historique, scientifique). Il s'agit de garantir le bon fonctionnement du secteur public et du secteur privé.

L'hypothèse de l'autorisation de la loi à enregistrer et communiquer des données est également exonératoire de l'obligation d'informer. On vise plus particulièrement ici le secteur public (paragraphe (3)).

ad Article 28

Le deuxième droit fondamental de toute personne est d'avoir accès aux données la concernant. Ce droit comporte différentes facettes:

– le droit d'obtenir la confirmation de l'existence d'un traitement, de même que les données traitées au sujet de la personne concernée, y compris la communication de ces données sous une forme intelligible;
– le droit de rectification, d'effacement ou de verrouillage des données dont le traitement n'est pas conforme à la présente loi, ainsi que
– le droit de disposer d'un recours.

Il est fondamental que le droit d'accès soit garanti et qu'il puisse s'exercer sans contrainte et sans frais, sous condition toutefois que la personne qui l'exerce soit en mesure de prouver son identité. En outre, le droit d'accès et le droit de rectification doivent pouvoir être exercés par un ayant droit de la

personne concernée, et ce dans la mesure où celui-ci prouve qu'il poursuit un intérêt légitime. En cas de litige, c'est à la Commission qu'il revient d'apprécier la légitimité de l'intérêt.

Il faut cependant distinguer entre l'intérêt légitime propre à l'ayant droit et l'intérêt légitime de la personne décédée que son héritier entend faire respecter. Par exemple: un fils peut avoir un intérêt légitime (propre) à accéder et à faire rectifier des données concernant son père qui seraient traitées dans un fichier bancaire. En effet, un questionnaire médical peut avoir été réalisé sur le père à l'ouverture d'un prêt (par exemple). Certaines de ces données peuvent avoir des retentissements négatifs sur l'octroi d'un prêt au fils. Ainsi des antécédents familiaux de maladies cardiaques ne font-ils jamais bonne impression auprès du banquier, alors qu'en réalité, le fils ne souffre d'aucune affection de ce type.

Les données collectées par un médecin; qu'elles soient à caractère particulier (article 6 (1) du projet de loi) ou anodines doivent être soumises au droit d'accès. Il s'agit d'une application de droit commun de la protection des données qui est en parfaite conformité avec l'article 36 de la loi du 28 août 1998 sur les établissements hospitaliers. L'article 28 paragraphe (4) règle le droit d'accès de toute personne aux données la concernant traitées à des fins de journalisme. Afin de ne pas mettre en cause les recherches du journaliste, il doit être dérogé au droit d'accès direct de la personne concernée.

Si, lors de l'exercice de son droit d'accès la personne concernée a de sérieux doutes quant à la conformité des données communiquées par rapport à celles qui seraient effectivement traitées, elle peut recourir à l'aide de la Commission.

Il est précisé au paragraphe (7), à l'instar de l'article 23 de la loi du 31 mars 1979, que si une rectification, un effacement ou un verrouillage de données sont effectués, ces modifications doivent, en principe, être notifiées aux tiers auxquels les données ont été communiquées.

ad Article 29

L'article 29 prévoit pour quelles raisons l'exercice du droit d'accès peut être refusé, limité ou différé par le responsable du traitement. Les exceptions au droit d'accès sont reprises de l'article 13 de la Directive. En dehors des attributs de la puissance publique (paragraphe (1) a) et d): sûreté, sécurité, activités pénales …), on y retrouve la protection de la personne concernée ou des droits et libertés d'autrui, ainsi que le cas dans lequel *„… il n'existe manifestement aucun risque d'atteinte à la vie privée d'une personne concernée, … lorsque les données sont traitées exclusivement aux fins de recherche scientifique ou sont stockées sous la forme de données à la seule finalité d'établissement de statistiques …"*.

Afin que ces exceptions ne soient pas appliquées de façon arbitraire, et que le recours au droit d'accès indirect demeure l'exception, le responsable du traitement doit informer la personne concernée du motif pour lequel il refuse, limite ou diffère l'exercice du droit en question, alors qu'il traite les données pour les finalités limitativement énoncées. Le cas échéant, il est obligé d'indiquer quand l'accès sera à nouveau possible (paragraphe (3)).

La personne concernée peut s'adresser à la Commission, pour que celle-ci procède, en son nom, aux vérifications nécessaires, tout en faisant opérer la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente loi. La Commission est en droit de communiquer à la personne concernée le résultat de ses investigations, notamment si les motifs invoqués par le responsable du traitement ne s'avèrent pas justifiés, mais ceci sans pouvoir mettre en danger la ou les finalités des traitements (paragraphe (4)).

ad Article 30

Il est créé dans le chef de la personne concernée, un nouveau droit, tel que prévu par l'article 14 de la Directive 95/46/CE, à savoir le droit d'opposition.

Ce droit peut être invoqué par toute personne concernée dans deux cas précis.

L'article 30 paragraphe (1) prévoit que la personne concernée peut, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, s'opposer à ce que ses données fassent l'objet d'un traitement, sauf en cas de disposition légale qui prévoit expressément le traitement. On vise ici tout particulièrement l'article 5 paragraphe (1) b) et d). La lettre b) de l'article 5 traite des activités d'utilité publique et de service public comme vecteur de la légitimité du traitement, tandis que la lettre d) de l'article 5 concerne l'intérêt légitime du responsable du traitement et vise par là le secteur privé en général. Ces cas se situent dans la droite ligne du principe de la libre circulation des données.

L'article 30 paragraphes (2) et (3) vise le traitement de données à caractère personnel à des fins de prospection, notamment commerciale, de même qu'en cas de communication de telles données à des tiers ou utilisées pour le compte de tiers aux mêmes fins, la personne concernée, dûment informée, peut s'opposer respectivement à ce traitement et à la communication, ainsi qu'à l'utilisation de ses données à des fins de prospection. Le droit d'opposition est inconditionnel.

ad Article 31

L'article 31 transpose l'article 15 de la Directive relatif aux décisions individuelles automatisées. Il instaure le droit de toute personne à ne pas être soumis à une décision individuelle automatisée (paragraphe (1). Il est fondamental que ce type de décisions ne porte pas atteinte à la vie privée des personnes concernées. Les principales applications de ce type particulier de décisions concernent essentiellement le credit-scoring et l'évaluation du personnel. De telles décisions individualisées visent par exemple l'appréciation du rendement de la personne concernée, l'évaluation de son crédit, l'appréciation de sa personnalité et l'analyse de son comportement (paragraphe (2)).

Chapitre VII. *Responsabilité et recours*

ad Article 32

Sans commentaire.

ad Article 33

La procédure décrite est une procédure rapide qui sanctionne les violations des formalités prévues par la loi. On s'est inspiré de la procédure d'urgence prévue dans la réglementation sur la profession de transporteur. Cette procédure rapide s'adapte à notre loi, dès lors qu'il s'agit de sanctionner rapidement les défauts patents de respect des formalités exigées préalablement à la mise en oeuvre d'un traitement.

On vise ici les formalités de publicité, de notification et le cas échéant celle de l'autorisation préalable qu'elle soit délivrée par la Commission (articles 14 et 16 de la loi) ou par règlement grand-ducal (article 17 de la loi). Les litiges au fond suivront le cours des procédures civiles et pénales classiques.

Il s'agit d'un instrument efficace combinant rapidité et caractère semi-inquisitorial (l'initiative appartient pour partie au ministère public) rappelant le caractère d'ordre public des règles élémentaires de protection des personnes concernées au regard de la libre circulation des données. Les parties civiles pourront être toute partie lésée, soit encore la personne concernée mais également toute autre personne ayant un intérêt à agir.

La rapidité de cette procédure permet:

– de rappeler aux acteurs de la loi que le cadre mis en place est contraignant et connaît des applications pratiques „douloureuses“ et immédiates. Ceci est nécessaire pour une meilleure prise de conscience de l'opinion publique alors que l'on sort d'un régime juridique peu actif;
– de permettre une réponse rapide aux abus manifestes dans l'environnement des nouvelles technologies qui est en perpétuel mouvement.

La nature de cette procédure:

– ne se substitue pas aux sanctions administratives que peut administrer la Commission. La Commission a un champ d'intervention plus large. En effet elle contrôle de façon approfondie le respect des règles de fond prévues dans la loi. La présente procédure ne sanctionne que la violation flagrante des formalités exigées et prévues par la loi et nécessaire à la mise en oeuvre d'un traitement;
– ne se substitue pas aux procédures des référés car il s'agit ici de sanctionner le responsable du traitement en le paralysant dans son activité (on vise ici particulièrement l'activité de commerce des données qui se développe) alors que le juge des référés recherche la conservation des droits des personnes concernées par le verrouillage, la destruction des données traitées, l'interdiction temporaire ou définitive du traitement réalisé en violation de la loi. De plus, il s'agit d'une procédure rapide et non d'urgence. L'action ne se heurtera donc pas à la condition de l'urgence lors de l'analyse de sa recevabilité.

Chapitre VIII. *Contrôle et surveillance de l'application de la loi*

La loi du 31 mars 1979 prévoyait un contrôle a priori systématique (avis de la commission consultative suivi de l'autorisation du ministre ayant dans ses attributions le répertoire national des banques de données) tandis que la Directive 95/46/CE qui repose sur la libre circulation des données assortie d'un contrôle a posteriori.

L'institution d'une autorité administrative indépendante, telle que prévue par l'article 28 de la Directive 95/46/CE, dispose d'un pouvoir de contrôle plus étendu que celui prévu par la loi du 31 mars 1979. Les pouvoirs d'investigation et d'intervention par tous moyens nécessaires pour pouvoir exercer en toute indépendance ses missions, seront à l'avenir le garant pour une application correcte de la présente loi.

L'indépendance est indispensable dans l'esprit de la Directive. Elle constitue une des pierres angulaires de la loi afin que fonctionne convenablement le principe du contrôle a posteriori et que soit sauvegardé le principe de la libre circulation des données. La Directive met en place un régime unique applicable aussi bien aux personnes publiques qu'aux personnes privées. La garantie d'indépendance de la Commission doit être aussi bien structurelle que fonctionnelle; ôter l'un ou l'autre de ces éléments reviendrait à retirer une béquille au nécessiteux. Toutefois, cette indépendance ne signifie pas que les pouvoirs qui lui sont attribués peuvent être exercés discrétionnairement. Toute décision de la Commission est susceptible de recours en justice de sorte que l'indépendance s'exerce de façon transparente et sous le contrôle du juge.

La transparence se traduit entre autres par la publication d'un rapport d'activité annuel adressé au Gouvernement (article 34 paragraphe (2)), la publication d'un rapport annuel qui fait état des notifications et autorisations (article 15 paragraphe (4)) ainsi que par la publication du règlement intérieur de la Commission au Mémorial (article 37 paragraphe (1)).

ad Article 34

Le paragraphe (1) dispose que la dénomination de l'autorité administrative indépendante est „Commission Nationale pour la Protection des Données". Cette dénomination est reprise de la traduction de la loi de transposition portugaise. Elle est en accord avec le rapport de Monsieur Guy Braibant qui suggère que l'on parle d'autorité de protection plutôt que d'autorité de contrôle „*le contrôle n'étant qu'un des moyens d'assurer la protection*".

Le paragraphe (2) impose la rédaction annuelle d'un rapport présenté au Conseil de Gouvernement. Le rapport annuel de l'article 34 paragraphe (2) diffère de celui de l'article 15 paragraphe (4) en ce sens que le rapport de l'article 34 est plus explicite. Il a pour objet de relever plus particulièrement les déficiences ou abus constatés et de souligner le cas échéant des questions de droit. Tandis que le rapport de l'article 15 n'est en fait qu'un relevé des notifications et autorisations dont toute personne intéressée peut gratuitement en prendre connaissance. Il s'agit d'une obligation de transparence inhérente à la mise en place d'une autorité administrative indépendante telle que prévue par la Directive.

Les missions de cette autorité de contrôle sont générales (paragraphe 3). Elle assure l'application des dispositions de la présente loi et de ses règlements d'exécution. Elle est chargée du contrôle a posteriori et le cas échéant a priori (article 14 de la loi) de tout traitement de données à caractère personnel effectué en exécution des dispositions de la présente loi.

A cet effet, la Commission:

– reçoit les notifications (article 15 de la directive) préalables à la mise en oeuvre d'un traitement, de même que les changements affectant le contenu des notifications, et assure la publicité de ces traitements en tenant le registre afférent;
– procède au contrôle de la licéité des traitements notifiés (article 28 paragraphes (1) et (4) de la Directive);
– émet les avis requis lors de l'autorisation préalable d'un traitement (article 28 paragraphe (2) de la Directive), les avis préalables à l'adoption de tout texte de loi, ainsi que de tout projet de modification d'une telle loi ou d'un tel règlement grand-ducal, de même que les avis préalables à tout projet d'interconnexion de traitements;
– approuve les codes de conduite relatifs à un traitement ou un ensemble de traitements (article 27 paragraphe (2) de la Directive) qui ne sont pas susceptibles de porter atteinte à la vie privée des

personnes concernées qui lui sont soumis par des associations professionnelles représentatives du secteur privé;

– conseille le Gouvernement 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 physiques, et peut, à cette fin, faire procéder à des études et à des enquêtes (article 27 paragraphe (2) de la Directive);
– favorise, enfin, la diffusion d'informations relatives aux droits des personnes concernées et aux obligations des responsables de traitement, notamment en ce qui concerne le transfert de données à caractère personnel vers des Etats tiers disposant ou ne disposant pas d'un niveau de protection adéquat.

Dans le cadre de ses missions, la Commission dispose d'une compétence spéciale (article 27 paragraphe (3) (e)) d'aviser préalablement tout règlement, toute loi portant création d'un traitement de données à caractère personnel. On interroge spécialement le Conseil d'Etat pour qu'il avise sur la qualité juridique de cette disposition. De l'avis des rédacteurs, la Commission n'étant pas une juridiction, il ne devrait pas y avoir de problème relativement à cette disposition.

Une autre mission de la Commission sera celle d'aider les personnes concernées dans l'exercice de leurs droits (article 28 paragraphe (4) de la Directive). A cette fin, elle pourra être saisie par toute personne d'une demande de vérification de la licéité d'un traitement de façon générale et en particulier, en cas de refus ou de limitation de l'exercice du droit d'accès conformément à l'article 29, paragraphe (4) du présent projet de loi.

Afin de faire respecter la présente loi la Commission dispose d'un pouvoir général d'investigation (article 28 paragraphe (3) de la directive) lui permettant d'avoir un accès direct aux locaux où a lieu le traitement et aux données faisant l'objet du traitement en question, et d'avoir communication de tous renseignements et documents nécessaires à l'accomplissement de sa mission.

Finalement, la Commission peut ester en justice (article 28 paragraphe (3) de la Directive). Ceci renvoit au recours de droit commun et à l'article 34. La Commission a également le devoir de dénoncer aux autorités judiciaires les infractions à la loi dont elle a connaissance.

La Commission étant une autorité administrative indépendante, les actes qu'elle adopte sont des actes administratifs. Si ces actes font grief, ils peuvent être attaqués devant les juridictions administratives: Le recours sera un recours en annulation de droit commun. Les règles de procédure et de délais applicables sont celles qui régissent ces juridictions.

Sur le plan international, il incombe à la Commission de coopérer avec ses „homologues" européens, de même que de représenter le Luxembourg dans les enceintes internationales, existantes et futures, instituées par des instruments juridiques internationaux.

ad Article 35

Les sanctions administratives (article 28 (3) de la Directive) sont prévues sans préjudice de toutes les autres sanctions pénales insérées dans le corps de la loi.

La Commission dispose d'un pouvoir d'intervention (article 28 (3) de la Directive) lui permettant d'ordonner notamment le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement.

ad Article 36

Le paragraphe (1) dispose que la Commission a la personnalité juridique. Cet attribut est nécessaire pour permettre à la Commission d'ester en justice mais aussi pour assurer son indépendance structurelle et fonctionnelle.

Le paragraphe (2) prévoit le nombre de 3 membres effectifs et de 3 membres suppléants dans la Commission. Ce nombre est impair ceci, afin de garantir une gestion collégiale. Le terme de 6 ans renouvelable une fois permet un certain renouveau dans la composition de la Commission et l'approche de ses membres face à une matière éminemment juridique et politique.

Le paragraphe (3) dispose que les membres (effectifs et suppléants) sont nommés par le Grand-Duc sur proposition du Gouvernement en conseil. Il faudra au moins un juriste et un informaticien, tous deux – comme tous les autres membres – devant être proposés en vue de leur compétence.

Le paragraphe (4) traite des incompatibilités entre la fonction qui leur est attribuée en qualité de membre de la Commission et leur fonction d'origine.

Le paragraphe (5) traite de la cessation de mandat et n'apporte pas de commentaire particulier (idem pour le paragraphe 6).

ad Article 37

Le paragraphe (1) dispose que la Commission établit son règlement intérieur ainsi que ses procédures et méthodes de travail dans le mois de son installation. Ceux-ci constituent les outils assurant l'indépendance de la Commission quant à son fonctionnement interne. Le délai de la mise en place est bref car on ne saurait laisser fonctionner la Commission assortie d'une large indépendance sans prévoir une présentation transparente de ses règles de fonctionnement. Ce qui justifie d'ailleurs sa publication au Mémorial (B).

Le paragraphe (2) traite du contenu de ce règlement.

Les paragraphes (3) et (4) et (6) ont trait à l'organisation interne de la Commission et n'appellent pas d'observations particulières.

Le paragraphe (5) traite les conflits d'intérêts. C'est la Commission qui apprécie dans chaque cas les conflits d'intérêts qu'elle peut opposer à ses membres (effectifs et suppléants). La Commission constate les cas d'empêchement et les conflits d'intérêts. Ceci est un élément important qui évite de mettre en cause son indépendance.

Le paragraphe (7) traite de la révocation des membres (effectifs et suppléants). Le Grand-Duc révoque sur proposition de l'autorité ayant proposé le membre en cause à la nomination, en l'occurrence le Gouvernement en conseil, ceci sur avis conforme de la Commission pris à la majorité des membres présents. Ce système permet de respecter le parallélisme des formes tout en garantissant l'indépendance de la Commission alors qu'elle émet un avis conforme à la proposition de révocation.

Quant au paragraphe (8) il permet d'éviter que les pouvoirs politiques n'interfèrent indirectement sur les activités des membres de la Commission.

ad Article 38

L'article 38 traite du cadre du personnel de la Commission. Les agents (environ 6 à 7 personnes) assisteront les membres de la Commission constituant l'organe collégial, dans l'exercice de leurs fonctions. Les agents et les membres ont la qualité d'employé privé à assimiler à des employés de l'Etat dont le cadre et les dispositions afférentes seront fixés par règlement grand-ducal.

Les paragraphes (4) et (5) rendent directement la commission débitrice des rémunérations de ses membres, agents, employés et ouvriers. Ceci n'est qu'un aspect de l'autonomie financière corollaire de l'autonomie administrative et nécessaire à son indépendance.

En revanche la Commission doit avoir une certaine flexibilité et doit recourir dans certains cas (ex. traitement de données relevant du domaine scientifique tel que le génie génétique etc.) à des experts externes (paragraphe 6).

ad Article 39

L'idée principale de cet article consiste à prévoir une indépendance financière pour un organe ne disposant pratiquement pas de ressources financières propres (exception: redevances perçues sur base de l'article 13 paragraphe 5). Le but est d'éviter d'introduire par le biais d'une tutelle financière une dépendance administrative. Dans cet ordre d'idées l'article 39 prévoit une dotation annuelle (à fixer) au budget de l'Etat qui constitue l'enveloppe budgétaire dont la gérance relève de la responsabilité des membres de la Commission.

Les dispositions sont reprises de la loi sur la Commission de surveillance du secteur financier.

ad Article 40

L'équilibre entre la libre circulation des données et la protection des personnes concernées exige que l'autorité de contrôle (Commission nationale pour la protection des données) soit dotée d'une indépendance structurelle et fonctionnelle importante.

Toutefois, la Directive prévoit que l'on peut substituer à la Commission „un détaché à la protection des données" (article 18 (2) de la Directive). L'instauration d'un „délégué à la protection des données"

(Datenschutzbeauftragter) est une pratique courante dans les entreprises allemandes. L'intérêt pratique de recourir à un détaché ou délégué à la protection des données au sein d'une entreprise peut consister d'une part à sensibiliser les salariés à la protection des données personnelles les concernant dont ils ne mesurent pas toujours l'importance et d'autre part à tenter de limiter l'ampleur bureaucratique du contrôle.

L'article 40 retient la possibilité offerte par la Directive de recourir à un détaché à la protection des données. Ce détaché est dénommé „chargé de la protection des données" dans le projet de loi. Cette institution se substitue à la Commission au stade de la notification en devenant le destinataire de celle-ci.

Ainsi, le chargé de la protection des données doit, à l'instar de la Commission, *„assurer de manière indépendante l'application interne des dispositions nationales prises en application de (…) la Directive (… et …) tenir un registre des traitements effectués par le responsable du traitement …"*[1]. Ces missions qui se substituent en grande partie à celles de la Commission ne peuvent être effectuées que de façon indépendante (article 40 paragraphe 4 du projet de loi et 18 paragraphe (2) tiret 3 de la Directive). La garantie de cette indépendance nécessite d'interdire tout lien de subordination entre le responsable du traitement et le chargé de la protection des données. Ainsi, ces deux acteurs ne pourront pas être liés par un contrat de travail alors qu'un des critères définissant ce type de contrat est l'existence même d'un lien de subordination.

L'indépendance du chargé de la protection des données est renforcée par l'octroi d'une protection accrue et de pouvoirs importants lors de l'accomplissement de ses missions (article 40 paragraphe (3)). En effet, celui-ci:

– ne peut être révoqué pour des raisons liées à l'exercice de ses missions, hormis le cas de la violation de ses obligations légales et/ou conventionnelles;
– dispose de tout pouvoir d'investigation afin d'assurer la surveillance du respect des dispositions de la présente loi et de ses règlements d'exécution par le responsable du traitement;
– dispose d'un droit d'information auprès du responsable du traitement et, corrélativement, d'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.

Dans l'esprit de la Directive, l'option laissée au responsable du traitement de désigner un chargé de la protection des données se substituant pour partie à la Commission a pour objectif de faciliter la gestion des traitements que le responsable met en oeuvre mais en aucun cas de diminuer les prérogatives de la Commission.

Ainsi, le chargé de la protection des données désigné par le responsable du traitement doit se comporter comme un conseil et un guide de l'application de la loi à son égard. Le chargé est un auxiliaire de la protection des données dans la mesure où il doit tout comme la Commission assurer l'application correcte des dispositions de la présente loi et de ses règlements d'exécution. Il détient également un registre des traitements effectués par le responsable du traitement qui est identique à celui tenu par la Commission quant à son contenu et son fonctionnement (article 40 paragraphe (2) a) et b)).

C'est encore en sa qualité d'auxiliaire de la protection des données qu'il est soumis au secret professionnel tout comme les membres et agents de la Commission (cf. article 24 du projet de loi).

Pour garantir l'indépendance du chargé de la protection des données dans l'exercice de ses missions celui-ci ne doit connaître aucun lien de subordination vis-à-vis du responsable du traitement (exclusion du contrat de travail).

L'article 40 paragraphe (5) dispose que le chargé consulte la Commission dès qu'il a un doute s'agissant de la conformité à la loi d'un traitement mis en oeuvre sous sa surveillance. Cette idée est reprise de l'article 20 paragraphe (2) de la directive.

Notons que le champ d'activité du chargé de la protection des données se limite au droit commun, c'est-à-dire au traitement soumis à la notification. En effet, il ne saurait être question de substituer le chargé de la protection des données à la Commission dans le cadre de la procédure d'autorisation préa-

1 Article 18 paragraphe (2) tirets 3 et 4 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données.

lable de l'article 14 ce qui conférerait à celui-ci un pouvoir d'édicter des actes administratifs individuels.

L'activité de chargé de la protection est ouverte aux professionnels du secteur de la protection des données par deux voies. Tout d'abord elle est accessible immédiatement pour certaines professions réglementées. Elle est en deuxième lieu accessible sur agrément de la Commission qui exige la preuve de l'obtention d'un titre universitaire et d'une assise financière de 15 millions de francs. Ces dispositions ont été reprises de la loi du 31 mai 1999 régissant la domiciliation des sociétés. Certaines adaptations ont cependant paru nécessaires. En effet, dans une matière touchant aux droits et libertés fondamentaux, il paraît souhaitable de garantir les qualités des chargés de la protection des données. Par exemple on a ajouté les médecins à la liste des professions réglementées ayant accès à cette activité de plein droit. Cette disposition vise particulièrement les données médicales traitées conformément à l'article 7 paragraphe (3) de la loi. De même, la liste des titres universitaires permettant d'obtenir l'agrément a été élargie aux diplômes des sciences de la nature ainsi qu'aux diplômes en informatique. Ces compétences pourront en effet, se révéler nécessaires à la bonne gestion des missions de chargé de la protection des données. En outre, la Commission pourra toujours s'opposer à la désignation d'un chargé de la protection qui n'aurait pas les qualités requises pour exercer cette fonction ou en cas de conflit d'intérêt, entre cette fonction et les relations préexistantes entre le responsable du traitement et le chargé désigné. Il s'agit ici de garantir l'indépendance du chargé de la protection des données en parant le risque d'influence entre lui et le responsable du traitement par exemple, lorsque ceux-ci sont en relations d'affaires continue et que ces relations d'affaires risqueraient d'entamer le crédit de la fonction de chargé de la protection des données. Enfin, la Commission mettra en place un contrôle continu sous forme de formations à valider pour parfaire l'exigence du contrôle des qualités requises de tout chargé de la protection des données. Ce système articule, libre initiative et garanties qualitatives au bénéfice des personnes concernées, mais aussi des responsables de traitements qui auront comme chargés de la protection des données, des interlocuteurs crédibles.

Chapitre IX. *Dispositions spécifiques; transitoires et finales*

ad Article 41

L'article 41 est une exception aux principes énoncés dans la présente loi dans la mesure où il oblige les opérateurs de télécommunications et/ou postaux ainsi que leurs fournisseurs de services de permettre l'accès à certaines données relatives à leurs abonnés et aux services de ceux-ci.

Suite à la libéralisation des télécommunications la présence sur le marché d'une multitude d'opérateurs et de fournisseurs de services a rendu de plus en plus difficile l'identification et la localisation d'une personne pour l'accomplissement d'une mission légale de surveillance (art. 88-1 et suivants du code d'instruction criminelle ainsi que le flagrant délit) ou d'une mission de sauvegarde de la vie humaine par les services de secours.

A l'heure actuelle l'exécution d'une mesure d'interception légale nécessite l'entrée en contact avec chaque opérateur (opérateur de réseau fixe ou mobile) ou prestataire de services pour se procurer des données relatives à la cible à intercepter. L'effort sera d'autant plus néfaste dans la mesure où le secret de l'opération risque d'être anéanti au regard du nombre croissant de personnes impliquées dans la détermination des moyens de communication d'une cible.

Les services de secours rencontrent des problèmes similaires dans la mesure où l'accès aux données d'une personne bénéficiaire d'un secours devient plus compliqué vu le nombre croissant d'opérateurs et/ou de fournisseurs de services.

Pour remédier à cette situation devenue difficilement gérable, l'article 41 paragraphe (1) tente d'apporter une solution pragmatique en s'inspirant du modèle néerlandais.

Confrontés aux mêmes problèmes, les Pays-Bas et l'Allemagne ont créé un „organisme indépendant" dénommé CIOT (= centre d'information) qui dispose d'un accès électronique aux bases de données „clients" des opérateurs et/ou des fournisseurs de services. Un tel centre vient d'être créé par une loi aux Pays-Bas. Ce système se limite pour l'instant à l'interception légale alors que l'article 41 paragraphe (1) a pour objet d'y inclure les missions de sauvegarde de la vie humaine.

Pour obtenir les renseignements nécessaires à la préparation des requêtes d'interception, les autorités légales s'adressent par voie électronique au centre d'information qui vérifie si le requérant est autorisé à formuler la requête d'où il transmet celle-ci à des systèmes informatiques appelés „boîtes noires" installées auprès des opérateurs et/ou fournisseurs de services. Sur demande du centre d'information la „boîte noire"

répond électroniquement si elle connaît ou non le nom du client en question et de quels services celui-ci dispose. La nature et le format des données doivent être définis de manière uniforme pour tous les opérateurs et/ou fournisseurs de services. Ces derniers doivent au moins une fois par jour mettre à jour leurs données contenues dans leur „boîte noire“. Les données doivent être accessibles 24 heures sur 24 et 7 jours sur 7. Par ce mécanisme, à l'exception de la mise à jour; l'opérateur et/ou le fournisseur de services n'est donc pas en mesure de savoir si une requête a été transmise ni à propos de quel client elle a été introduite.

Les avantages d'un tel système:

La discrétion et la confidentialité sont garanties:

a) d'une part par un ou plusieurs fonctionnaires assermentés qui traitent les requêtes introduites dans le cadre de l'article 41 ainsi que par la communication semestrielle du registre des requêtes à la Commission permettant ainsi un contrôle de la légalité des requêtes d'information et la prévention d'abus éventuels;
b) d'autre part si la procédure est automatisée (article 41 paragraphe (4)) celle-ci permettra l'accès par voie électronique sans intervention manuelle de sorte que l'opérateur ignore quand l'accès à sa boîte noire est exercé.

L'approche constitue donc une version électronique de la procédure actuelle, c.-à-d. les mêmes données communiquées à l'heure actuelle par voie administrative seront transmises électroniquement aux autorités de l'Etat. En principe, les procédures sont maintenues, mais leur exécution se fait dorénavant par voie électronique. Le „centre d'information“ ne dispose d'aucune base de données centralisée laquelle est remplacée par le mécanisme des requêtes en temps réel ce qui permet par exemple de gagner du temps précieux dans le cas d'une prise d'otage.

Les coûts sont assez réduits ainsi après un investissement initial, les coûts d'exploitation sont très réduits par rapport à la démarche actuelle intense en ressources humaines.

L'article 41 paragraphe (1) vise donc à conférer le rôle du centre d'information à l'ILR du fait qu'il est en contact direct avec les opérateurs et/ou les fournisseurs de services des télécommunications et/ou postaux. L'ILR aura seul accès aux données de la „boîte noire“ ce qui permet de centraliser et de retracer les requérants. Les données doivent être à jour et l'accès doit être permanent. Un règlement grand-ducal détermine la nature et le format des données contenus dans la „boîte noire“ ainsi que la structure et le fonctionnement du système.

Afin d'éviter des abus, le paragraphe (2) prend soin de bien délimiter le champ d'application de l'accès. Pour éviter qu'en matière de sauvegarde de la vie privée, des services de secours non clairement identifiés puissent avoir accès, il est prévu qu'un code de conduite définit le type, les conditions d'accès ainsi que la ou les catégories de personnes autorisées à avoir accès.

Le paragraphe (3) énonce la procédure applicable en ce qui concerne l'exécution des requêtes.

Le paragraphe (4) prévoit la possibilité d'automatiser la procédure dont les avantages ont été exposés ci-dessus.

Le paragraphe (5) est une précision essentielle dans la mesure où elle interdit l'utilisation des données de la „boîte noire“ pour un nouveau traitement de données qui seraient ainsi dépourvues de leur finalité primaire. Pour des raisons de transparence, il faut que l'ILR tienne un registre des requêtes qui est communiqué à la Commission pour vérification en cas d'irrégularités.

ad Article 42

Sans commentaire.

ad Article 43

Sans commentaire.

ad Article 44

La présente loi abroge la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, telle qu'elle a été modifiée par les lois des 19 novembre 1987, 30 septembre 1992, 1er octobre 1992 et 9 août 1993 et ses règlements afférents tels que:

(a) le règlement grand-ducal du 2 août 1979 organisant la Commission consultative prévue à l'article 30 de la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques;

(b) le règlement grand-ducal du 13 avril 1984 portant exécution des articles 19 et 20 de la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques;

(c) le règlement grand-ducal du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale telle que modifiée par le règlement grand-ducal du 9 août 1993;

(d) le règlement grand-ducal du 2 octobre 1992 réglementant l'utilisation des données nominatives médicales dans les traitements informatiques;

(e) le règlement grand-ducal du 9 août 1993 relatif à l'organisation et au fonctionnement de la Commission prévue au paragraphe (4) de l'article 12-1 de la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques.

ad Article 45

Sans commentaire.

*

DIRECTIVE 95/46/CE DU PARLEMENT EUROPEEN 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

LE PARLEMENT EUROPEEN ET LE CONSEIL DE L'UNION EUROPEENNE,

vu le traité instituant la Communauté européenne, et notamment son article 100 A, vu la proposition de la Commission[(1)],

vu l'avis du Comité économique et social[(2)],

statuant conformément à la procédure visée à l'article 189 B du traité[(3)],

(1) considérant que les objectifs de la Communauté, énoncés dans le traité, tel que modifié par le traité sur l'Union européenne, consistent à réaliser une union sans cesse plus étroite entre les peuples européens, à établir des relations plus étroites entre les Etats que la Communauté réunit, à assurer par une action commune le progrès économique et social en éliminant les barrières qui divisent l'Europe, à promouvoir l'amélioration constante des conditions de vie de ses peuples, à préserver et conforter la paix et la liberté, et à promouvoir la démocratie en se fondant sur les droits fondamentaux reconnus dans les constitutions et les lois des Etats membres, ainsi que dans la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales;

(2) considérant que les systèmes de traitement de données sont au service de l'homme; qu'ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus;

(3) considérant que l'établissement et le fonctionnement du marché intérieur dans lequel, conformément à l'article 7 A du traité, la libre circulation des marchandises, des personnes, des services et des capitaux est assurée, nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un Etat membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés;

---

(1)JO No C 277 du 5.11.1990, p. 3.
JO No C 311 du 27.11.1992, p. 30.

(2)JO No C 159 du 17.6.1991, p. 38.

(3)Avis du Parlement européen du 11 mars 1992 (JO No C 94 du 13.4.1992, p. 198), confirmé le 2 décembre 1993 (JO No C 342 du 20.12.1993, p. 30); position commune du Conseil du 20 février 1995 (JO No C 93 du 13.4.1995, p. 1) et décision du Parlement européen du 15 juin 1995 (JO No C 166 du 3.7.1995).

(4) considérant que, dans la Communauté, il est fait de plus en plus fréquemment appel au traitement de données à caractère personnel dans les divers domaines de l'activité économique et sociale; que les progrès des technologies de l'information facilitent considérablement le traitement et l'échange de ces données;

(5) considérant que l'intégration économique et sociale résultant de l'établissement et du fonctionnement du marché intérieur au sens de l'article 7 A du traité va nécessairement entraîner une augmentation sensible des flux transfrontaliers de données à caractère personnel entre tous les acteurs de la vie économique et sociale des Etats membres, que ces acteurs soient privés ou publics; que l'échange de données à caractère personnel entre des entreprises établies dans des Etats membres différents est appelé à se développer; que les administrations des Etats membres sont appelées, en application du droit communautaire, à collaborer et à échanger entre elles des données à caractère personnel afin de pouvoir accomplir leur mission ou exécuter des tâches pour le compte d'une administration d'un autre Etat membre, dans le cadre de l'espace sans frontières que constitue le marché intérieur;

(6) considérant, en outre, que le renforcement de la coopération scientifique et technique ainsi que la mise en place coordonnée de nouveaux réseaux de télécommunications dans la Communauté nécessitent et facilitent la circulation transfrontalière de données à caractère personnel;

(7) considérant que les différences entre Etats membres quant au niveau de protection des droits et libertés des personnes, notamment du droit à la vie privée, à l'égard des traitements de données à caractère personnel peuvent empêcher la transmission de ces données du territoire d'un Etat membre à celui d'un autre Etat membre; que ces différences peuvent dès lors constituer un obstacle à l'exercice d'une série d'activités économiques à l'échelle communautaire, fausser la concurrence et empêcher les administrations de s'acquitter des responsabilités qui leur incombent en vertu du droit communautaire; que ces différences de niveau de protection résultent de la disparité des dispositions nationales législatives, réglementaires et administratives;

(8) considérant que, pour éliminer les obstacles à la circulation des données à caractère personnel, le niveau de protection des droits et libertés des personnes à l'égard du traitement de ces données doit être équivalent dans tous les Etats membres; que cet objectif, fondamental pour le marché intérieur, ne peut pas être atteint par la seule action des Etats membres, compte tenu en particulier de l'ampleur des divergences qui existent actuellement entre les législations nationales applicables en la matière et de la nécessité de coordonner les législations des Etats membres pour que le flux transfrontalier de données à caractère personnel soit réglementé d'une manière cohérente et conforme à l'objectif du marché intérieur au sens de l'article 7 A du traité; qu'une intervention de la Communauté visant à un rapprochement des législations est donc nécessaire;

(9) considérant que, du fait de la protection équivalente résultant du rapprochement des législations nationales, les Etats membres ne pourront plus faire obstacle à la libre circulation entre eux de données à caractère personnel pour des raisons relatives à la protection des droits et libertés des personnes, notamment du droit à la vie privée; que les Etats membres disposeront d'une marge de manoeuvre qui, dans le contexte de la mise en oeuvre de la directive, pourra être utilisée par les partenaires économiques et sociaux; qu'ils pourront donc préciser, dans leur législation nationale, les conditions générales de licéité du traitement des données; que, ce faisant, les Etats membres s'efforceront d'améliorer la protection assurée actuellement par leur législation; que, dans les limites de cette marge de manoeuvre et conformément au droit communautaire, des disparités pourront se produire dans la mise en oeuvre de la directive et que cela pourra avoir des incidences sur la circulation des données tant à l'intérieur d'un Etat membre que dans la Communauté;

(10) considérant que l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire; que, pour cette raison, le rapprochement de ces législations ne doit pas conduire à affaiblir la protection qu'elles assurent mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans la Communauté;

(11) considérant que les principes de la protection des droits et des libertés des personnes, notamment du droit à la vie privée, contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la convention, du 28 janvier 1981, du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel;

(12) considérant que les principes de la protection doivent s'appliquer à tout traitement de données à caractère personnel dès lors que les activités du responsable du traitement relèvent du champ d'application du droit communautaire; que doit être exclu le traitement de données effectué par une personne physique dans l'exercice d'activités exclusivement personnelles ou domestiques, telles la correspondance et la tenue de répertoires d'adresses;

(13) considérant que les activités visées aux titres V et VI du traité sur l'Union européenne concernant la sécurité publique, la défense, la sûreté de l'Etat ou les activités de l'Etat dans le domaine pénal ne relèvent pas du champ d'application du droit communautaire, sans préjudice des obligations incombant aux Etats membres au titre de l'article 56 paragraphe 2 et des articles 57 et 100 A du traité; que le traitement de données à caractère personnel qui est nécessaire à la sauvegarde du bien-être économique de l'Etat ne relève pas de la présente directive lorsque ce traitement est lié à des questions de sûreté de l'Etat;

(14) considérant que, compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données;

(15) considérant que les traitements portant sur de telles données ne sont couverts par la présente directive que s'ils sont automatisés ou si les données sur lesquelles ils portent sont contenues ou sont destinées à être contenues dans un fichier structuré selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause;

(16) considérant que les traitements des données constituées par des sons et des images, tels que ceux de vidéosurveillance, ne relèvent pas du champ d'application de la présente directive s'ils sont mis en oeuvre à des fins de sécurité publique, de défense, de sûreté de l'Etat ou pour l'exercice des activités de l'Etat relatives à des domaines du droit pénal ou pour l'exercice d'autres activités qui ne relèvent pas du champ d'application du droit communautaire;

(17) considérant que, pour ce qui est des traitements de sons et d'images mis en oeuvre à des fins de journalisme ou d'expression littéraire ou artistique, notamment dans le domaine audiovisuel, les principes de la directive s'appliquent d'une manière restreinte selon les dispositions prévues à l'article 9;

(18) considérant qu'il est nécessaire, afin d'éviter qu'une personne soit exclue de la protection qui lui est garantie en vertu de la présente directive, que tout traitement de données à caractère personnel effectué dans la Communauté respecte la législation de l'un des Etats membres; que, à cet égard, il est opportun de soumettre les traitements de données effectués par toute personne opérant sous l'autorité du responsable du traitement établi dans un Etat membre à l'application de la législation de cet Etat;

(19) considérant que l'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable; que la forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard; que, lorsqu'un même responsable est établi sur le territoire de plusieurs Etats membres, en particulier par le biais d'une filiale, il doit s'assurer, notamment en vue d'éviter tout contournement, que chacun des établissements remplit les obligations prévues par le droit national applicable aux activités de chacun d'eux;

(20) considérant que l'établissement, dans un pays tiers, du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive; que, dans ce cas, il convient de soumettre les traitements de données effectués à la loi de l'Etat membre dans lequel des moyens utilisés pour le traitement de données en cause sont localisés et de prendre des garanties pour que les droits et obligations prévus par la présente directive soient effectivement respectés;

(21) considérant que la présente directive ne préjuge pas des règles de territorialité applicables en matière de droit pénal;

(22) considérant que les Etats membres préciseront dans leur législation ou lors de la mise en oeuvre des dispositions prises en application de la présente directive les conditions générales dans lesquelles le traitement de données est licite; que, en particulier, l'article 5, en liaison avec les articles 7 et 8, permet aux Etats membres de prévoir, indépendamment des règles générales, des conditions particulières pour les traitements de données dans des secteurs spécifiques et pour les différentes catégories de données visées à l'article 8;

(23) considérant que les Etats membres sont habilités à assurer la mise en oeuvre de la protection des personnes, tant par une loi générale relative à la protection des personnes à l'égard du traitement des données à caractère personnel que par des lois sectorielles telles que celles relatives par exemple aux instituts de statistiques;

(24) considérant que les législations relatives à la protection des personnes morales à l'égard du traitement des données qui les concernent ne sont pas affectées par la présente directive;

(25) considérant que les principes de la protection doivent trouver leur expression, d'une part, dans les obligations mises à la charge des personnes, autorités publiques, entreprises, agences ou autres organismes qui traitent des données, ces obligations concernant en particulier la qualité des données, la sécurité technique, la notification à l'autorité de contrôle, les circonstances dans lesquelles le traitement peut être effectué, et, d'autre part, dans les droits donnés aux personnes dont les données font l'objet d'un traitement d'être informées sur celui-ci, de pouvoir accéder aux données, de pouvoir demander leur rectification, voire de s'opposer au traitement dans certaines circonstances;

(26) considérant que les principes de la protection doivent s'appliquer à toute information concernant une personne identifiée ou identifiable; que, pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en oeuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne; que les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable; que les codes de conduite au sens de l'article 27 peuvent être un instrument utile pour fournir des indications sur les moyens par lesquels les données peuvent être rendues anonymes et conservées sous une forme ne permettant plus l'identification de la personne concernée;

(27) considérant que la protection des personnes doit s'appliquer aussi bien au traitement de données automatisé qu'au traitement manuel; que le champ de cette protection ne doit pas en effet dépendre des techniques utilisées, sauf à créer de graves risques de détournement; que, toutefois, s'agissant du traitement manuel, la présente directive ne couvre que les fichiers et ne s'applique pas aux dossiers non structurés; que, en particulier, le contenu d'un fichier doit être structuré selon des critères déterminés relatifs aux personnes permettant un accès facile aux données à caractère personnel; que, conformément à la définition figurant à l'article 2 point c), les différents critères permettant de déterminer les éléments d'un ensemble structuré de données à caractère personnel et les différents critères régissant l'accès à cet ensemble de données peuvent être définis par chaque Etat membre; que les dossiers ou ensembles de dossiers, de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés n'entrent en aucun cas dans le champ d'application de la présente directive;

(28) considérant que tout traitement de données à caractère personnel doit être effectué licitement et loyalement à l'égard des personnes concernées; qu'il doit, en particulier, porter sur des données adéquates, pertinentes et non excessives au regard des finalités poursuivies; que ces finalités doivent être explicites et légitimes et doivent être déterminées lors de la collecte des données; que les finalités des traitements ultérieurs à la collecte ne peuvent pas être incompatibles avec les finalités telles que spécifiées à l'origine;

(29) considérant que le traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques n'est pas considéré en général comme incompatible avec les finalités pour

lesquelles les données ont été auparavant collectées, dans la mesure où les Etats membres prévoient des garanties appropriées; que ces garanties doivent notamment empêcher l'utilisation des données à l'appui de mesures ou de décisions prises à l'encontre d'une personne;

(30) considérant que, pour être licite, un traitement de données à caractère personnel doit en outre être fondé sur le consentement de la personne concernée ou être nécessaire à la conclusion ou à l'exécution d'un contrat liant la personne concernée, ou au respect d'une obligation légale, ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, ou encore à la réalisation d'un intérêt légitime d'une personne à condition que ne prévalent pas l'intérêt ou les droits et libertés de la personne concernée; que, en particulier, en vue d'assurer l'équilibre des intérêts en cause, tout en garantissant une concurrence effective, les Etats membres peuvent préciser les conditions dans lesquelles des données à caractère personnel peuvent être utilisées et communiquées à des tiers dans le cadre d'activités légitimes de gestion courante des entreprises et autres organismes; que, de même, ils peuvent préciser les conditions dans lesquelles la communication à des tiers de données à caractère personnel peut être effectuée à des fins de prospection commerciale, ou de prospection faite par une association à but caritatif ou par d'autres associations ou fondations, par exemple à caractère politique, dans le respect de dispositions visant à permettre aux personnes concernées de s'opposer sans devoir indiquer leurs motifs et sans frais au traitement des données les concernant;

(31) considérant qu'un traitement de données à caractère personnel doit être également considéré comme licite lorsqu'il est effectué en vue de protéger un intérêt essentiel à la vie de la personne concernée;

(32) considérant qu'il appartient aux législations nationales de déterminer si le responsable du traitement investi d'une mission d'intérêt public ou d'une mission relevant de l'exercice de l'autorité publique doit être une administration publique ou une autre personne soumise au droit public ou au droit privé, telle qu'une association professionnelle;

(33) considérant que les données qui sont susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée ne devraient pas faire l'objet d'un traitement, sauf consentement explicite de la personne concernée; que, cependant, des dérogations à cette interdiction doivent être expressément prévues pour répondre à des besoins spécifiques, en particulier lorsque le traitement de ces données est mis en oeuvre à certaines fins relatives à la santé par des personnes soumises à une obligation de secret professionnel ou pour la réalisation d'activités légitimes par certaines associations ou fondations dont l'objet est de permettre l'exercice de libertés fondamentales;

(34) considérant que les Etats membres doivent également être autorisés à déroger à l'interdiction de traiter des catégories de données sensibles lorsqu'un motif d'intérêt public important le justifie dans des domaines tels que la santé publique et la protection sociale – particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie – et tels que la recherche scientifique et les statistiques publiques; qu'il leur incombe, toutefois, de prévoir les garanties appropriées et spécifiques aux fins de protéger les droits fondamentaux et la vie privée des personnes;

(35) considérant, en outre, que le traitement de données à caractère personnel par des autorités publiques pour la réalisation de fins prévues par le droit constitutionnel ou le droit international public, au profit d'associations à caractère religieux officiellement reconnues, est mis en oeuvre pour un motif d'intérêt public important;

(36) considérant que, si, dans le cadre d'activités liées à des élections, le fonctionnement du système démocratique suppose, dans certains Etats membres, que les partis politiques collectent des données relatives aux opinions politiques des personnes, le traitement de telles données peut être autorisé en raison de l'intérêt public important, à condition que des garanties appropriées soient prévues;

(37) considérant que le traitement de données à caractère personnel à des fins de journalisme ou d'expression artistique ou littéraire, notamment dans le domaine audiovisuel, doit bénéficier de dérogations ou de limitations de certaines dispositions de la présente directive dans la mesure où elles sont

nécessaires à la conciliation des droits fondamentaux de la personne avec la liberté d'expression, et notamment la liberté de recevoir ou de communiquer des informations, telle que garantie notamment à l'article 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales; qu'il incombe donc aux Etats membres, aux fins de la pondération entre les droits fondamentaux, de prévoir les dérogations et limitations nécessaires en ce qui concerne les mesures générales relatives à la légalité du traitement des données, les mesures relatives au transfert des données vers des pays tiers ainsi que les compétences des autorités de contrôle, sans qu'il y ait lieu toutefois de prévoir des dérogations aux mesures visant à garantir la sécurité du traitement; qu'il conviendrait également de conférer au moins à l'autorité de contrôle compétente en la matière certaines compétences a posteriori, consistant par exemple à publier périodiquement un rapport ou à saisir les autorités judiciaires;

(38) considérant que le traitement loyal des données suppose que les personnes concernées puissent connaître l'existence des traitements et bénéficier, lorsque des données sont collectées auprès d'elles, d'une information effective et complète au regard des circonstances de cette collecte;

(39) considérant que certains traitements portent sur des données que le responsable n'a pas collectées directement auprès de la personne concernée; que, par ailleurs, des données peuvent être légitimement communiquées à un tiers, alors même que cette communication n'avait pas été prévue lors de la collecte des données auprès de la personne concernée; que, dans toutes ces hypothèses, l'information de la personne concernée doit se faire au moment de l'enregistrement des données ou, au plus tard, lorsque les données sont communiquées pour la première fois à un tiers;

(40) considérant que, cependant, il n'est pas nécessaire d'imposer cette obligation si la personne concernée est déjà informée; que, en outre, cette obligation n'est pas prévue si cet enregistrement ou cette communication sont expressément prévus par la loi ou si l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés, ce qui peut être le cas pour des traitements à des fins historiques, statistiques ou scientifiques; que, à cet égard, peuvent être pris en considération le nombre de personnes concernées, l'ancienneté des données, ainsi que les mesures compensatrices qui peuvent être prises;

(41) considérant que toute personne doit pouvoir bénéficier du droit d'accès aux données la concernant qui font l'objet d'un traitement, afin de s'assurer notamment de leur exactitude et de la licéité de leur traitement; que, pour les mêmes raisons, toute personne doit en outre avoir le droit de connaître la logique qui sous-tend le traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 15 paragraphe 1; que ce droit ne doit pas porter atteinte au secret des affaires ni à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel; que cela ne doit toutefois pas aboutir au refus de toute information de la personne concernée;

(42) considérant que les Etats membres peuvent, dans l'intérêt de la personne concernée ou en vue de protéger les droits et libertés d'autrui, limiter les droits d'accès et d'information; qu'ils peuvent, par exemple, préciser que l'accès aux données à caractère médical ne peut être obtenu que par l'intermédiaire d'un professionnel de la santé;

(43) considérant que des restrictions aux droits d'accès et d'information, ainsi qu'à certaines obligations mises à la charge du responsable du traitement de données, peuvent également être prévues par les Etats membres dans la mesure où elles sont nécessaires à la sauvegarde, par exemple, de la sûreté de l'Etat, de la défense, de la sécurité publique, d'un intérêt économique ou financier important d'un Etat membre ou de l'Union européenne, ainsi qu'à la recherche et à la poursuite d'infractions pénales ou de manquements à la déontologie des professions réglementées; qu'il convient d'énumérer, au titre des exceptions et limitations, les missions de contrôle, d'inspection ou de réglementation nécessaires dans les trois derniers domaines précités concernant la sécurité publique, l'intérêt économique ou financier et la répression pénale; que cette énumération de missions concernant ces trois domaines n'affecte pas la légitimité d'exceptions et de restrictions pour des raisons de sûreté de l'Etat et de défense;

(44) considérant que les Etats membres peuvent être amenés, en vertu de dispositions du droit communautaire, à déroger aux dispositions de la présente directive concernant le droit d'accès, l'information des personnes et la qualité des données, afin de sauvegarder certaines finalités parmi celles visées ci-dessus;

(45) considérant que, dans le cas où des données pourraient faire l'objet d'un traitement licite sur le fondement d'un intérêt public, de l'exercice de l'autorité publique ou de l'intérêt légitime d'une personne, toute personne concernée devrait, toutefois, avoir le droit de s'opposer, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que les données la concernant fassent l'objet d'un traitement; que les Etats membres ont, néanmoins, la possibilité de prévoir des dispositions nationales contraires;

(46) considérant que la protection des droits et libertés des personnes concernées à l'égard du traitement de données à caractère personnel exige que des mesures techniques et d'organisation appropriées soient prises tant au moment de la conception qu'à celui de la mise en oeuvre du traitement, en vue d'assurer en particulier la sécurité et d'empêcher ainsi tout traitement non autorisé; qu'il incombe aux Etats membres de veiller au respect de ces mesures par les responsables du traitement; que ces mesures doivent assurer un niveau de sécurité approprié tenant compte de l'état de l'art et du coût de leur mise en oeuvre au regard des risques présentés par les traitements et de la nature des données à protéger;

(47) considérant que, lorsqu'un message contenant des données à caractère personnel est transmis via un service de télécommunications ou de courrier électronique dont le seul objet est de transmettre des messages de ce type, c'est la personne dont émane le message, et non celle qui offre le service de transmission, qui sera normalement considérée comme responsable du traitement de données à caractère personnel contenues dans le message; que, toutefois, les personnes qui offrent ces services seront normalement considérées comme responsables du traitement des données à caractère personnel supplémentaires nécessaires au fonctionnement du service;

(48) considérant que la notification à l'autorité de contrôle a pour objet d'organiser la publicité des finalités du traitement, ainsi que de ses principales caractéristiques, en vue de son contrôle au regard des dispositions nationales prises en application de la présente directive;

(49) considérant que, afin d'éviter des formalités administratives inadéquates, des exonérations ou des simplifications de la notification peuvent être prévues par les Etats membres pour les traitements de données qui ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées, à condition qu'ils soient conformes à un acte pris par l'Etat membre qui en précise les limites; que des exonérations ou simplifications peuvent pareillement être prévues par les Etats membres dès lors qu'une personne désignée par le responsable du traitement de données s'assure que les traitements effectués ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées; que la personne ainsi détachée à la protection des données, employée ou non du responsable du traitement de données, doit être en mesure d'exercer ses fonctions en toute indépendance;

(50) considérant que des exonérations ou simplifications peuvent être prévues pour le traitement de données dont le seul but est de tenir un registre destiné, dans le respect du droit national, à l'information du public et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime;

(51) considérant que, néanmoins, le bénéfice de la simplification ou de l'exonération de l'obligation de notification ne dispense le responsable du traitement de données d'aucune des autres obligations découlant de la présente directive;

(52) considérant que, dans ce contexte, le contrôle a posteriori par les autorités compétentes doit être en général considéré comme une mesure suffisante;

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

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

(55) considérant que, en cas de non-respect des droits des personnes concernées par le responsable du traitement de données, un recours juridictionnel doit être prévu par les législations nationales; que les dommages que peuvent subir les personnes du fait d'un traitement illicite doivent être réparés par le responsable du traitement de données, lequel peut être exonéré de sa responsabilité s'il prouve que le fait dommageable ne lui est pas imputable, notamment lorsqu'il établit l'existence d'une faute de la personne concernée ou d'un cas de force majeure; que des sanctions doivent être appliquées à toute personne, tant de droit privé que de droit public, qui ne respecte pas les dispositions nationales prises en application de la présente directive;

(56) considérant que des flux transfrontaliers de données à caractère personnel sont nécessaires au développement du commerce international; que la protection des personnes garantie dans la Communauté par la présente directive ne s'oppose pas aux transferts de données à caractère personnel vers des pays tiers assurant un niveau de protection adéquat; que le caractère adéquat au niveau de protection offert par un pays tiers doit s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts;

(57) considérant, en revanche, que, lorsqu'un pays tiers n'offre pas un niveau de protection adéquat, le transfert de données à caractère personnel vers ce pays doit être interdit;

(58) considérant que des exceptions à cette interdiction doivent pouvoir être prévues dans certaines circonstances lorsque la personne concernée a donné son consentement, lorsque le transfert est nécessaire dans le contexte d'un contrat ou d'une action en justice, lorsque la sauvegarde d'un intérêt public important l'exige, par exemple en cas d'échanges internationaux de données entre les administrations fiscales ou douanières ou entre les services compétents en matière de sécurité sociale, ou lorsque le transfert est effectué à partir d'un registre établi par la loi et destiné à être consulté par le public ou par des personnes ayant un intérêt légitime; que, dans ce cas, un tel transfert ne devrait pas porter sur la totalité des données ni sur des catégories de données contenues dans ce registre; que, lorsqu'un registre est destiné à être consulté par des personnes qui ont un intérêt légitime, le transfert ne devrait pouvoir être effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires;

(59) considérant que des mesures particulières peuvent être prises pour pallier l'insuffisance du niveau de protection dans un pays tiers lorsque le responsable du traitement présente des garanties appropriées; que, en outre, des procédures de négociation entre la Communauté et les pays tiers en cause doivent être prévues;

(60) considérant que, en tout état de cause, les transferts vers les pays tiers ne peuvent être effectués que dans le plein respect des dispositions prises par les Etats membres en application de la présente directive, et notamment de son article 8;

(61) considérant que les Etats membres et la Commission, dans leurs domaines de compétence respectifs, doivent encourager les milieux professionnels concernés à élaborer des codes de conduite en vue de favoriser, compte tenu des spécificités du traitement de données effectué dans certains secteurs, la mise en oeuvre de la présente directive dans le respect des dispositions nationales prises pour son application;

(62) considérant que l'institution, dans les Etats membres, d'autorités de contrôle exerçant en toute indépendance leurs fonctions est un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel;

(63) considérant que ces autorités doivent être dotées des moyens nécessaires à l'exécution de leurs tâches, qu'il s'agisse des pouvoirs d'investigation et d'intervention, en particulier lorsque les autorités sont saisis de réclamations, ou du pouvoir d'ester en justice; qu'elles doivent contribuer à la transparence du traitement de données effectué dans l'Etat membre dont elles relèvent;

(64) considérant que les autorités des différents Etats membres seront appelées à se prêter mutuellement assistance dans la réalisation de leurs tâches afin d'assurer le plein respect des règles de protection dans l'Union européenne;

(65) considérant que, au niveau communautaire, un groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel doit être instauré et qu'il doit exercer ses fonctions en toute indépendance; que, compte tenu de cette spécificité, il doit conseiller la Commission et contribuer notamment à l'application homogène des règles nationales adoptées en application de la présente directive;

(66) considérant que, pour ce qui est du transfert de données vers les pays tiers, l'application de la présente directive nécessite l'attribution de compétences d'exécution à la Commission et l'établissement d'une procédure selon les modalités fixées dans la décision 87/373/CEE du Conseil[(1)];

(67) considérant qu'un accord sur un modus vivendi concernant les mesures d'exécution des actes arrêtés selon la procédure visée à l'article 189 B du traité est intervenu, le 20 décembre 1994, entre le Parlement européen, le Conseil et la Commission;

(68) considérant que les principes énoncés dans la présente directive et régissant la protection des droits et des libertés des personnes, notamment du droit à la vie privée, à l'égard du traitement des données à caractère personnel pourront être complétés ou précisés, notamment pour certains secteurs, par des règles spécifiques conformes à ces principes;

(69) considérant qu'il convient de laisser aux Etats membres un délai ne pouvant pas excéder trois ans à compter de l'entrée en vigueur des mesures nationales de transposition de la présente directive, pour leur permettre d'appliquer progressivement à tout traitement de données déjà mis en oeuvre les nouvelles dispositions nationales susvisées; que, afin de permettre un bon rapport coût-efficacité lors de la mise en oeuvre de ces dispositions, les Etats membres sont autorisés à prévoir une période supplémentaire, expirant douze ans après la date d'adoption de la présente directive, pour la mise en conformité des fichiers manuels existants avec certaines dispositions de la directive; que, lorsque des données contenues dans de tels fichiers font l'objet d'un traitement manuel effectif pendant cette période transitoire supplémentaire, la mise en conformité avec ces dispositions doit être effectuée au moment de la réalisation de ce traitement;

(70) considérant qu'il n'y a pas lieu que la personne concernée donne à nouveau son consentement pour permettre au responsable de continuer à effectuer, après l'entrée en vigueur des dispositions nationales prises en application de la présente directive, un traitement de données sensibles nécessaire à l'exécution d'un contrat conclu sur la base d'un consentement libre et informé avant l'entrée en vigueur des dispositions précitées;

(71) considérant que la présente directive ne s'oppose pas à ce qu'un Etat membre réglemente les activités de prospection commerciale visant les consommateurs qui résident sur son territoire, dans la mesure où cette réglementation ne concerne pas la protection des personnes à l'égard du traitement de données à caractère personnel;

(72) considérant que la présente directive permet de prendre en compte, dans la mise en oeuvre des règles qu'elle pose, le principe du droit d'accès du public aux documents administratifs,

ONT ARRETE LA PRESENTE DIRECTIVE:

---

(1)JO No L 197 du 18.7.1987, p. 33.

Chapitre premier – *Dispositions générales*

Article premier

Objet de la directive

1. Les Etats membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.

2. Les Etats membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre Etats membres pour des raisons relatives à la protection assurée en vertu du paragraphe 1.

Article 2

Définitions

Aux fins de la présente directive, on entend par:

a) „données à caractère personnel": toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale;

b) „traitement de données à caractère personnel" (traitement): toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, 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, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction;

c) „fichier de données à caractère personnel" (fichier): tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

d) „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 des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire;

e) „sous-traitement": la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

f) „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, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données;

g) „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 dans le cadre d'une mission d'enquête particulière ne sont toutefois pas considérées comme des destinataires;

h) „consentement de la personne concernée": toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Article 3

Champ d'application

1. La présente directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. La présente directive ne s'applique pas au traitement de données à caractère personnel:
   – mis en oeuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'Etat (y compris le bien-être économique de l'Etat lorsque ces traitements sont liés à des questions de sûreté de l'Etat) et les activités de l'Etat relatives à des domaines du droit pénal,
   – effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.

Article 4

Droit national applicable

1. Chaque Etat membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque:
   a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Etat membre; si un même responsable du traitement est établi sur le territoire de plusieurs Etats membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable;
   b) le responsable du traitement n'est pas établi sur le territoire de l'Etat membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public;
   c) le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit Etat membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté.

2. Dans le cas visé au paragraphe 1 point c), le responsable du traitement doit désigner un représentant établi sur le territoire dudit Etat membre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même.

Chapitre II – *Conditions générales de licéité des traitements de données à caractère personnel*

Article 5

Les Etats membres précisent, dans les limites des dispositions du présent chapitre, les conditions dans lesquelles les traitements de données à caractère personnel sont licites.

Section I. Principes relatifs à la qualité des données

Article 6

1. Les Etats membres prévoient que les données à caractère personnel doivent être:
   a) traitées loyalement et licitement;
   b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les Etats membres prévoient des garanties appropriées;
   c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;

d) exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;

e) 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 ou pour lesquelles elles sont traitées ultérieurement. Les Etats membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.

2. Il incombe au responsable du traitement d'assurer le respect du paragraphe 1.

Section II. Principes relatifs à la légitimation des traitements de données

Article 7

Les Etats membres prévoient que le traitement des données à caractère personnel ne peut être effectué que si:

a) la personne concernée a indubitablement donné son consentement

ou

b) 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

c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis

ou

d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée

ou

e) 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 tiers auquel les données sont communiquées

ou

f) 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 paragraphe 1.

Section III. Catégories particulières de traitements

Article 8

Traitements portant sur des catégories particulières de données

1. Les Etats membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.

2. Le paragraphe 1 ne s'applique pas lorsque:

a) la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'Etat membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée

ou

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 une législation nationale prévoyant des garanties adéquates

ou

c) le traitement est nécessaire à la défense 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

d) le traitement est effectué dans le cadre de leurs activités légitimes et avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux 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

e) le traitement porte sur des données manifestement rendues publiques par la personne concernée ou est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.

3. Le paragraphe 1 ne s'applique pas lorsque le traitement des données est 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 et que le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente.

4. Sous réserve de garanties appropriées, les Etats membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle.

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

Les Etats membres peuvent prévoir que les données relatives aux sanctions administratives ou aux jugements civils sont également traitées sous le contrôle de l'autorité publique.

6. Les dérogations au paragraphe 1 prévues aux paragraphes 4 et 5 sont notifiées à la Commission.

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

Article 9

Traitements de données à caractère personnel et liberté d'expression

Les Etats membres prévoient, pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations au présent chapitre, au chapitre IV et au chapitre VI dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression.

Section IV. Information de la personne concernée

Article 10

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

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

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

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

c) toute information supplémentaire telle que:

– les destinataires ou les catégories de destinataires des données,

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

– l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,

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

Article 11

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

1. Lorsque les données n'ont pas été collectées auprès de la personne concernée, les Etats membres prévoient que le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée:

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

b) les finalités du traitement;

c) toute information supplémentaire telle que:

– les catégories de données concernées,

– les destinataires ou les catégories de destinataires des données,

– l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,

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

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

Section V. Droit d'accès de la personne concernée aux données

Article 12

Droit d'accès

Les Etats membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement:

a) sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs:

– 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, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées,

– la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données,

– 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 15 paragraphe 1;

b) selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données;

c) la notification aux tiers auxquels les données ont été communiquées de toute rectification, tout effacement ou tout verrouillage effectué conformément au point b), si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné.

Section VI. Exceptions et limitations

Article 13

Exceptions et limitations

1. Les Etats membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 paragraphe 1, à l'article 10, à l'article 11 paragraphe 1 et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder:

a) la sûreté de l'Etat;

b) la défense;

c) la sécurité publique;

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

e) un intérêt économique ou financier important d'un Etat membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;

f) 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);

g) la protection de la personne concernée ou des droits et libertés d'autrui.

2. Sous réserve de garanties légales appropriées, excluant notamment que les données puissent être utilisées aux fins de mesures ou de décisions se rapportant à des personnes précises, les Etats membres peuvent, dans le cas où il n'existe manifestement aucun risque d'atteinte à la vie privée de la personne concernée, limiter par une mesure législative les droits prévus à l'article 12 lorsque les données sont traitées exclusivement aux fins de la recherche scientifique ou sont stockées sous la forme de données à caractère personnel pendant une durée n'excédant pas celle nécessaire à la seule finalité d'établissement de statistiques.

Section VII. Droit d'opposition de la personne concernée

Article 14

Droit d'opposition de la personne concernée

Les Etats membres reconnaissent à la personne concernée le droit:

a) au moins dans les cas visés à l'article 7 points e) et f), 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 disposition contraire du droit national. En cas d'opposition justifiée, le traitement mis en oeuvre par le responsable du traitement ne peut plus porter sur ces données;

b) de s'opposer, sur demande et gratuitement, au traitement des données à caractère personnel la concernant envisagé par le responsable du traitement à des fins de prospection

ou

d'être informée avant que des données à caractère personnel 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.

Les Etats membres prennent les mesures nécessaires pour garantir que les personnes concernées ont connaissance de l'existence du droit visé au point b) premier alinéa.

Article 15

Décisions individuelles automatisées

1. Les Etats membres reconnaissent à toute personne le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc.

2. Les Etats membres prévoient, sous réserve des autres dispositions de la présente directive, qu'une personne peut être soumise à une décision telle que celle visée au paragraphe l si une telle 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, telles que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime

ou

b) est autorisée par une loi qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

Section VIII. Confidentialité et sécurité des traitements

Article 16

Confidentialité des traitements

Toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales.

Article 17

Sécurité des traitements

1. Les Etats membres prévoient que le responsable du traitement doit mettre en oeuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel 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.

Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en oeuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

2. Les Etats membres prévoient que le responsable du traitement, lorsque le traitement est effectué pour son compte, 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 et qu'il doit veiller au respect de ces mesures.

3. La réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que:

– le sous-traitant n'agit que sur la seule instruction du responsable du traitement,

– les obligations visées au paragraphe 1, telles que définies par la législation de l'Etat membre dans lequel le sous-traitant est établi, incombent également à celui-ci.

4. Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures visées au paragraphe 1 sont consignés par écrit ou sous une autre forme équivalente.

Section IX. Notification

Article 18

Obligation de notification à l'autorité de contrôle

1. Les Etats membres prévoient que le responsable du traitement, ou le cas échéant son représentant, doit adresser une notification à l'autorité de contrôle visée à l'article 28 préalablement à la mise en oeuvre d'un traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées.

2. Les Etats membres ne peuvent prévoir de simplification de la notification ou de dérogation à cette obligation que dans les cas et aux conditions suivants:

– lorsque, pour les catégories de traitement qui, compte tenu des données à traiter, ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées, ils précisent les finalités des traitements, les données ou catégories de données traitées, la ou les catégories de personnes concernées, les destinataires ou catégories de destinataires auxquels les données sont communiquées et la durée de conservation des données

et/ou

– lorsque le responsable du traitement désigne, conformément au droit national auquel il est soumis, un détaché à la protection des données à caractère personnel chargé notamment:
  – d'assurer, d'une manière indépendante, l'application interne des dispositions nationales prises en application de la présente directive,
  – de tenir un registre des traitements effectués par le responsable du traitement, contenant les informations visées à l'article 21 paragraphe 2,

  et garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte faux droits et libertés des personnes concernées.

3. Les Etats membres peuvent prévoir que le paragraphe 1 ne s'applique pas aux traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

4. Les Etats membres peuvent prévoir une dérogation à l'obligation de notification ou une simplification de la notification pour les traitements visés à l'article 8 paragraphe 2 point d).

5. Les Etats membres peuvent prévoir que les traitements non automatisés de données à caractère personnel, ou certains d'entre eux, font l'objet d'une notification, éventuellement simplifiée.

Article 19

Contenu de la notification

1. Les Etats membres précisent les informations qui doivent figurer dans la notification. Elles comprennent au minimum:

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

b) la ou les finalités du traitement;

c) une description de la ou des catégories de personnes concernées et des données ou des catégories de données s'y rapportant;

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

e) les transferts de données envisagés à destination de pays tiers;

f) une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement en application de l'article 17.

2. Les Etats membres précisent les modalités de notification à l'autorité de contrôle des changements affectant les informations visées au paragraphe 1.

Article 20

Contrôles préalables

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

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

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

Article 21

Publicité des traitements

1. Les Etats membres prennent des mesures pour assurer la publicité des traitements.

2. Les Etats membres prévoient que l'autorité de contrôle tient un registre des traitements notifiés en vertu de l'article 18.

Le registre contient au minimum les informations énumérées à l'article 19 paragraphe 1 points a) à e).

Le registre peut être consulté par toute personne.

3. En ce qui concerne les traitements non soumis à notification, les Etats membres prévoient que le responsable du traitement ou une autre instance qu'ils désignent communique sous une forme appropriée à toute personne qui en fait la demande au moins les informations visées à l'article 19 paragraphe 1 points a) à e).

Les Etats membres peuvent prévoir que la présente disposition ne s'applique pas aux traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

Chapitre III – *Recours juridictionnels, responsabilité et sanctions*

Article 22

Recours

Sans préjudice du recours administratif qui peut être organisé, notamment devant l'autorité de contrôle visée à l'article 28, antérieurement à la saisine de l'autorité judiciaire, les Etats membres prévoient que toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question.

Article 23

Responsabilité

1. Les Etats membres prévoient que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi.

2. Le responsable du traitement peut être exonéré partiellement ou totalement de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

Article 24

Sanctions

Les Etats membres prennent les mesures appropriées pour assurer la pleine application des dispositions de la présente directive et déterminent notamment les sanctions à appliquer en cas de violation des dispositions prises en application de la présente directive.

Chapitre IV – *Transfert de données à caractère personnel vers des pays tiers*

Article 25

Principes

1. Les Etats membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat.

2. Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.

3. Les Etats membres et la Commission s'informent mutuellement des cas dans lesquels ils estiment qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2.

4. Lorsque la Commission constate, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2 du présent article, les Etats membres prennent les mesures nécessaires en vue d'empêcher tout transfert de même nature vers le pays tiers en cause.

5. La Commission engage, au moment opportun, des négociations en vue de remédier à la situation résultant de la constatation faite en application du paragraphe 4.

6. La Commission peut constater, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers assure un niveau de protection adéquat au sens du paragraphe 2 du présent article, en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l'issue des négociations visées au paragraphe 5, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes.

Les Etats membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

Article 26

Dérogations

1. Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers, les Etats membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2 peut être effectué, à condition que:

a) la personne concernée ait indubitablement donné son consentement au transfert envisagé

ou

b) le transfert soit nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement 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

f) le transfert intervienne au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

2. Sans préjudice du paragraphe 1, un Etat membre peut autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2, 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, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées.

3. L'Etat membre informe la Commission et les autres Etats membres des autorisations qu'il accorde en application du paragraphe 2.

En cas d'opposition exprimée par un autre Etat membre ou par la Commission et dûment justifiée au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, la Commission arrête les mesures appropriées, conformément à la procédure prévue à l'article 31 paragraphe 2.

Les Etats membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

4. Lorsque la Commission décide, conformément à la procédure prévue à l'article 31 paragraphe 2, que certaines clauses contractuelles types présentent les garanties suffisantes visées au paragraphe 2, les Etats membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

Chapitre V – *Codes de conduite*

Article 27

1. Les Etats membres et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales prises par les Etats membres en application de la présente directive.

2. Les Etats membres prévoient que les associations professionnelles et les autres organisations représentant d'autres catégories de responsables du traitement qui ont élaboré des projets de codes nationaux ou qui ont l'intention de modifier ou de proroger des codes nationaux existants peuvent les soumettre à l'examen de l'autorité nationale.

Les Etats membres prévoient que cette autorité s'assure, entre autres, de la conformité des projets qui lui sont soumis avec les dispositions nationales prises en application de la présente directive. Si elle l'estime opportun, l'autorité recueille les observations des personnes concernées ou de leurs représentants.

3. Les projets de codes communautaires, ainsi que les modifications ou prorogations de codes communautaires existants, peuvent être soumis au groupe visé à l'article 29. Celui-ci se prononce, entre autres, sur la conformité des projets qui lui sont soumis avec les dispositions nationales prises en application de la présente directive. S'il l'estime opportun, il recueille les observations de personnes concernées ou de leurs représentants. La Commission peut assurer une publicité appropriée aux codes qui ont été approuvés par le groupe.

Chapitre VI – *Autorité de contrôle et groupe de protection des personnes à l'égard du traitement des données à caractère personnel*

Article 28

Autorité de contrôle

1. Chaque Etat membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les Etats membres en application de la présente directive.

Ces autorités exercent en toute indépendance les missions dont elles sont investies.

2. Chaque Etat membre prévoit que les autorités de contrôle sont consultées lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel.

3. Chaque autorité de contrôle dispose notamment:

– de pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle,

– de pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en oeuvre des traitements, conformément à l'article 20, et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ou celui de saisir les parlements nationaux ou d'autres institutions politiques,

– du pouvoir d'ester en justice en cas de violation des dispositions nationales prises en application de la présente directive ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire.

Les décisions de l'autorité de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel.

4. Chaque autorité de contrôle peut être saisie par toute personne, ou par une association la représentant, d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel. La personne concernée est informée des suites données à sa demande.

Chaque autorité de contrôle peut, en particulier, être saisie par toute personne d'une demande de vérification de la licéité d'un traitement lorsque les dispositions nationales prises en vertu de l'article 13 de la présente directive sont d'application. La personne est à tout le moins informée de ce qu'une vérification a eu lieu.

5. Chaque autorité de contrôle établit à intervalles réguliers un rapport sur son activité. Ce rapport est publié.

6. Indépendamment du droit national applicable au traitement en cause, chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'Etat membre dont elle relève, les pouvoirs dont elle est investie conformément au paragraphe 3. Chaque autorité peut être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre Etat membre.

Les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant toute information utile.

7. Les Etats membres prévoient que les membres et agents des autorités de contrôle sont soumis, y compris après cessation de leurs activités, à l'obligation du secret professionnel à l'égard des informations confidentielles auxquelles ils ont accès.

Article 29

Groupe de protection des personnes à l'égard du traitement des données à caractère personnel

1. Il est institué un groupe de protection des personnes à l'égard du traitement des données à caractère personnel, ci-après dénommé „groupe".

Le groupe a un caractère consultatif et indépendant.

2. Le groupe se compose d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque Etat membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission.

Chaque membre du groupe est désigné par l'institution, l'autorité ou les autorités qu'il représente. Lorsqu'un Etat membre a désigné plusieurs autorités de contrôle, celles-ci procèdent à la nomination d'un représentant commun. Il en va de même pour les autorités créées pour les institutions et organismes communautaires.

3. Le groupe prend ses décisions à la majorité simple des représentants des autorités de contrôle.

4. Le groupe élit son président. La durée du mandat du président est de deux ans. Le mandat est renouvelable.

5. Le secrétariat du groupe est assuré par la Commission.

6. Le groupe établit son règlement intérieur.

7. Le groupe examine les questions mises à l'ordre du jour par son président, soit à l'initiative de celui-ci, soit à la demande d'un représentant des autorités de contrôle ou de la Commission.

Article 30

1. Le groupe a pour mission:

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

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

2. Si le groupe constate que des divergences, susceptibles de porter atteinte à l'équivalence de la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté, s'établissent entre les législations et pratiques des Etats membres, il en informe la Commission.

3. Le groupe peut émettre de sa propre initiative des recommandations sur toute question concernant la protection des personnes à l'égard du traitement de données à caractère personnel dans la Communauté.

4. Les avis et recommandations du groupe sont transmis à la Commission et au comité visé à l'article 31.

5. La Commission informe le groupe des suites qu'elle a données à ses avis et recommandations. Elle rédige à cet effet un rapport qui est transmis également au Parlement européen et au Conseil. Ce rapport est publié.

6. Le groupe établit un rapport annuel sur l'état de la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans la Communauté et dans les pays tiers, qu'il communique à la Commission, au Parlement européen et au Conseil. Ce rapport est publié.

Chapitre VII – *Mesures d'exécution communautaires*

Article 31

Comité

1. La Commission est assistée par un comité composé des représentants des Etats membres et présidé par le représentant de la Commission.

2. Le représentant de la Commission soumet au comité un projet des mesures à prendre. Le comité émet son avis sur ce projet, dans un délai que le président peut fixer en fonction de l'urgence de la question en cause.

L'avis est émis à la majorité prévue à l'article 148 paragraphe 2 du traité. Lors des votes au sein du comité, les voix des représentants des Etats membres sont affectées de la pondération définie à l'article précité. Le président ne prend pas part au vote.

La Commission arrête des mesures qui sont immédiatement applicables. Toutefois, si elles ne sont pas conformes à l'avis émis par le comité, ces mesures sont aussitôt communiquées par la Commission au Conseil. Dans ce cas:

– la Commission diffère l'application des mesures décidées par elle d'un délai de trois mois à compter de la date de la communication,
– le Conseil, statuant à la majorité qualifiée, peut prendre une décision différente dans le délai prévu au premier tiret.

Dispositions finales

Article 32

1. Les Etats membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard à l'issue d'une période de trois ans à compter de son adoption.

Lorsque les Etats membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les Etats membres.

2. Les Etats membres veillent à ce que les traitements dont la mise en oeuvre est antérieure à la date d'entrée en vigueur des dispositions nationales prises en application de la présente directive soient rendus conformes à ces dispositions au plus tard trois ans après cette date.

Par dérogation à l'alinéa précédent, les Etats membres peuvent prévoir que les traitements de données déjà contenues dans des fichiers manuels à la date d'entrée en vigueur des dispositions nationales prises en application de la présente directive seront rendus conformes aux articles 6, 7 et 8 de la présente directive dans un délai de douze ans à compter de la date d'adoption de celle-ci. Les Etats membres permettent toutefois à la personne concernée d'obtenir, à sa demande et notamment lors de l'exercice du droit d'accès, la rectification, l'effacement ou le verrouillage des données incomplètes, inexactes ou conservées d'une manière qui est incompatible avec les fins légitimes poursuivies par le responsable du traitement.

3. Par dérogation au paragraphe 2, les Etats membres peuvent prévoir, sous réserve des garanties appropriées, que les données conservées dans le seul but de la recherche historique ne soient pas rendues conformes aux articles 6, 7 et 8 de la présente directive.

4. Les Etats membres communiquent à la Commission le texte des dispositions de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 33

Périodiquement, et pour la première fois au plus tard trois ans après la date prévue à l'article 32 paragraphe 1, la Commission fait un rapport au Parlement européen et au Conseil sur l'application de la présente directive et l'assortit, le cas échéant, des propositions de modification appropriées. Ce rapport est publié.

La Commission examine, en particulier, l'application de la présente directive aux traitements de données constituées par des sons et des images, relatives aux personnes physiques, et elle présente les propositions appropriées qui pourraient s'avérer nécessaires en tenant compte des développements de la technologie de l'information et à la lumière de l'état des travaux sur la société de l'information.

Article 34

Les Etats membres sont destinataires de la présente directive.

FAIT à Luxembourg, le 24 octobre 1995.

Par le Parlement européen,
Le président,
K. HAENSCH

Par le Conseil,
Le président,
L. ATIENZA SERNA

*

EXPOSE DES MOTIFS

Table des matières de l'exposé des motifs

I Historique

I.1. La loi de 1979

I.2. L'évolution informatique des vingt dernières années

I.3. Le nouveau droit communautaire

I.4. Du principe de l'autorisation préalable au principe de la libre circulation

I.5. La genèse du présent projet de loi

II Les objectifs du présent projet de loi

II.1. Libre circulation et protection des droits des personnes

II.2. Un champ d'application précisant et dépassant celui de la directive

II.3. Une loi-cadre

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

b) La liste des règlements grand-ducaux

II.4. L'importance du projet de loi pour la protection des droits et libertés fondamentaux, et particulier de la vie privée

II.5. Une loi importante pour le développement du monde économique

a) Un complément indispensable à la loi relative au commerce électronique et aux besoins du commerce électronique

b) La place financière

II.6. Une loi devant améliorer l'utilisation des banques de données publiques

a) L'amélioration du fonctionnement des administrations publiques

b) La préservation de l'activité régulière de l'administration

c) Les impératifs liés à la puissance publique

III Résumé des principales dispositions de la loi

III.1. La donnée

a) La définition: art. 2(a)

b) Les caractéristiques de qualité du traitement des données (article 4 de la loi);

III.2. Le traitement

a) Définition (art. 3 paragraphe (1))

b) Les traitements exclus: les activités personnelles ou domestiques (art. 3 paragraphe (3))

c) La légitimité de la personne mettant en oeuvre un traitement (article 5)

d) Les conditions de mise en oeuvre d'un traitement

e) Les droits de la personne concernée

III.3. Les catégories particulières de traitements

A Le traitement de catégories particulières de données dites encore données sensibles

a) L'interdiction de principe

b) Les exceptions générales (l'article 6 paragraphe (2))

c) Les procédures judiciaires: les besoins de la bonne administration de la justice
d) Les données génétiques (article 6 paragraphe (3) et (4) et article 7)

B Le traitement de catégories particulières de données par les services de la santé (article 7):
a) Les cas d'ouverture
b) Les personnes autorisées
c) Les modalités de la mise en oeuvre

C Les données judiciaires (article 8)

D Les traitements de données et la liberté d'expression (article 9)
a) Définition
b) Limitation et exception des droits d'information et d'accès
c) La notification allégée

E Les traitements à des fins de surveillance (article 10)
a) Les cas prévus
b) La garantie supplémentaire: l'information spéciale
c) Une communication limitée des données issues de la surveillance

F La surveillance sur le lieu de travail (article 11)
a) Les cas d'ouverture
b) la garantie supplémentaire: l'information spéciale
c) Le régime de mise en oeuvre

G Le cas spécial du répertoire téléphonique (article 41)

III.4. Les procédures
a) Les exemptions à l'obligation de notification (article 12 paragraphe (2))
b) La notification (art. 12, 13)
c) L'autorisation préalable (article 14)
d) L'autorisation préalable par voie de règlement grand-ducal (art. 17)

III.5. La commission nationale pour la protection des données
a) Le statut et l'indépendance
b) Le chargé de la protection des données (article 40)
c) La composition de la commission (article 36)
d) Les missions de la Commission (article 34)
e) Les pouvoirs (articles 34 et 35)

III.6. Les recours
a) La Commission
b) Les recours de droit commun (article 32)
c) Le recours rapide spécifique (article 33)
d) Les sanctions pénales

III.7. Le transfert vers des pays tiers (articles 18 à 20)

Conclusion

*

I. HISTORIQUE

Le présent projet de loi transpose en droit national 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. Cette Directive[1] fait suite chronologiquement sur le plan international à la Convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite encore Convention 108 du Conseil de l'Europe.

I.1. La loi de 1979

En approuvant en mars 1979 le projet de loi réglementant l'utilisation des données nominatives dans les traitements informatiques, le Luxembourg rejoignait alors le cercle restreint des pays dotés d'une législation en la matière. Après la Suède (Data Act de 1973), la République fédérale d'Allemagne (Bundesdatenschutzgesetz de 1977), le Canada (Human Rights Act de 1977), la France (Loi relative à l'informatique, aux fichiers et aux libertés de 1978), la Norvège, le Danemark et l'Autriche (également en 1978), le Luxembourg devenait le huitième pays à se doter d'une loi „protection des données".

La notion de „protection des données", constitue en fait un usage linguistique incorrect. L'objet de la législation en la matière n'est point de „protéger les données à caractère personnel" mais de garantir le respect des libertés et droits fondamentaux des personnes, et notamment de leur vie privée à l'égard du traitement automatisé des données les concernant. Cette idée est reflétée par le titre de la nouvelle loi. Toutefois, afin de ne pas alourdir le texte de l'exposé des motifs et du commentaire des articles, l'usage de la notion de „protection des données" y sera généralement maintenu.

Les mesures adoptées par le législateur de 1979 avaient pour objet d'assurer une meilleure protection contre une éventuelle utilisation abusive de données nominatives. Elles soumettaient toute création et toute exploitation d'une banque de données nominatives à l'autorisation préalable. Cette autorisation était octroyée respectivement par la loi ou par règlement grand-ducal pour les banques de données relevant de l'Etat et par arrêté ministériel pour celles ne relevant pas de l'Etat, sur avis d'une commission consultative qui examinait individuellement les demandes d'autorisation introduites.

Vu le nombre restreint de banques de données exploitées à la fin des années soixante-dix et au début des années quatre-vingt ce raisonnement inclus dans la loi de 1979, était adapté à son époque. Voilà pourquoi, le législateur était d'avis qu'il fallait un régime unique[2] et qu'il ne fallait pas tenir compte de la nature spécifique de certains traitements de données.

Dans son avis du 7 novembre 1978, le Conseil d'Etat soutient cette approche et expose en substance qu'eu égard au risque d'atteinte à la vie privée, la création et l'exploitation des banques de données devra être soumise à une autorisation préalable.

Le Conseil d'Etat approuve encore les auteurs du projet de loi de n'avoir pas confié à un organisme spécial la mission d'autoriser ou non la création et l'exploitation des banques de données du secteur privé. En effet, le nombre relativement peu élevé des demandes en autorisation à décider ne justifiait pas le création d'un tel organisme[3] (voir document parlementaire No 2131[1], session ordinaire 1977-1978, page 4).

Finalement, la commission spéciale de la Chambre des Députés, dans son avis du 27 février 1979, *„approuve avec le Conseil d'Etat le fait que le principe de l'autorisation préalable ait été généralisé pour le motif qu'il est difficile en pratique d'établir des critères objectifs permettant d'établir deux procédures distinctes: autorisation préalable et simple déclaration"*[4].

Ainsi chaque banque de données devait être examinée et autorisée individuellement avant sa mise en service. Aux termes des textes belges et français, ce contrôle est toujours assuré par un nouvel organisme public jouissant d'un statut propre et d'une certaine autonomie vis-à-vis du Gouvernement. Pour

1 JOCE No L 281/31, le 23.11.1995

2 On peut s'interroger sur la structure du régime d'autorisation, qui connaissait des procédures diversifiées qui étaient fonctions de la nature publique ou privée du responsable du traitement.

3 La pratique a singulièrement démenti cette affirmation.

4 Document parlementaire No 2131[2], session ordinaire 1977-1978, page 8

des raisons d'ordre administratif et financier, le projet luxembourgeois ne prévoyait donc pas la création d'un tel organisme[1].

I.2. L'évolution informatique des vingt dernières années

L'environnement informatique de l'époque se caractérisait par l'existence, surtout dans le secteur public, de quelques ordinateurs centralisés. C'était l'ère des systèmes macroinformatiques dans les grandes organisations et dans les administrations publiques. A cette époque, l'informatique est l'affaire de quelques spécialistes, mal connue et peu diffusée dans le grand public; … le PC n'était pas encore inventé! L'ordinateur était avant tout utilisé comme instrument qui permettait d'améliorer les relations entre l'administration et ses administrés et ceci dans un souci de plus grande efficacité.

Le raisonnement qui était à la base de cette première législation (cf. supra) en matière de protection des données, partait des trois hypothèses suivantes:

„erstens, die feste Überzeugung, daß die Verwendung von Computern notwendigerweise dazu führen muß, die Verarbeitung personenbezogener Daten in immer größeren Datenbanken zu zentralisieren;

zweitens, die Erwartung, daß sich die Automatisierung, allein schon wegen der damit verbundenen Kosten, auf die Verarbeitung der Daten einzelner, aus der Perspektive der öffentlichen Verwaltung besonders wichtiger Personengruppen konzentrieren würde;

sowie, drittens, die Vorstellung, daß verbindliche Verarbeitungsvorgaben zwar nicht ausschließlich, aber doch weitgehend nur bei staatlichen Datensammlungen vonnöten seien."[2]

Trois hypothèses qui se sont avérées erronées!

1. Le phénomène de la miniaturisation, la micro-informatique, de même que celui de l'interconnexion de banques de données moyennant la création systématique de réseaux, ont pris la relève des „gros" calculateurs et des banques de données volumineuses, entraînant une délocalisation des traitements et une décentralisation des données (plusieurs milliers de PC auprès de l'Etat).

2. Le traitement automatisé de données à caractère personnel a débuté, pour des raisons de rentabilité, par des traitements relatifs à des groupes importants de personnes (sécurité sociale, contributions, permis de conduire). Toutefois, l'évolution de la technologie, d'une part, la diminution de son coût, de l'autre, ont permis d'aboutir au „tout informatique". Le traitement manuel des données constitue dorénavant l'exception.

3. Le traitement de données à caractère personnel n'est plus un domaine réservé à l'Etat. Le développement rapide de la micro-informatique a changé le monde de l'informatique. Le citoyen passif, mis en fiches par les grandes organisations et les administrations, est devenu un utilisateur actif des moyens informatiques, depuis la carte de crédit jusqu'au poste multimédia, personnel ou professionnel. Les entreprises privées, les associations sans but lucratif et les autres groupements de personnes traitent quotidiennement des données à caractère personnel. Ainsi on est passé d'une société dans laquelle l'informatique était un outil au service des activités humaines à une société de l'information entraînant des modifications structurelles de nos modes de vie.

4. L'informatique est devenue un instrument indispensable dans la vie quotidienne des acteurs sociaux. Les bases de données sont désormais transmises d'un bout à l'autre du globe par téléchargement. De puissants moteurs de recherche permettent de réaliser des croisements et des synthèses de fichiers, sans recourir à une nomenclature commune. L'interconnexion et le traitement de masse des données sont une réalité. En même temps, la nature des données personnelles susceptibles d'être traitées s'est diversifiée et contient non seulement le son et l'image mais aussi les empreintes digitales ou le génome humain, de sorte que la quantité d'informations recueillies sur chaque individu devient de plus en plus importante.

---

1 Les fonctions de contrôle sont exercées cumulativement par une Commission consultative mixte et le ministre ayant dans ses attributions le répertoire national des banques de données (voir document parlementaire N° 2131, session ordinaire 1977-1978, page 9). Notons que la Directive 95/46 impose la création d'un tel organisme de droit public.

2 Article du professeur Spiros Simitis „Das scheinbar Private ist längst öffentlich", paru dans „Frankfurter Rundschau" du 19 juin 1995.

Ainsi cette évolution dans le domaine de l'informatique a bouleversé considérablement les enjeux en matière de protection des données à caractère personnel. C'est la combinaison des facteurs que sont:

1) La démocratisation de l'outil informatique communiquant (PC multimédia);

2) L'accroissement de la vitesse de traitement de l'information;

3) L'accroissement des capacités de stockage et des capacités de communication;

qui ont causé l'obsolescence de la loi du 31 mars 1979, telle qu'elle a été modifiée par la suite, au point qu'elle est devenue quasiment inapplicable.

A plusieurs reprises, le Gouvernement a eu l'intention de proposer des modifications, dans le sens d'une „adaptation" de ses dispositions à un environnement informatique évolué, sans pour autant mettre en cause les principes mêmes de la protection des données.

I.3. Le nouveau droit communautaire

Toutefois, aucune réforme substantielle et suffisante n'a été entreprise depuis une décennie. La raison en est simple: la Commission européenne présenta un paquet de mesures, dont l'objet était d'harmoniser dans les Etats membres de l'Union européenne les législations en matière de protection des données, afin que celles-ci ne soient plus à l'origine de restrictions ou d'interdictions à la libre circulation des données à caractère personnel dans le marché unique.

L'intervention au niveau communautaire était d'autant plus utile que la possibilité de transmettre des données d'un bout à l'autre du globe, ainsi que le développement de „réseaux universels" rendent vaine une protection limitée au cadre national. Des disparités trop importantes entre les législations existantes ont favorisé le phénomène de la délocalisation des traitements et des bases de données, de sorte qu'un des objectifs du paquet consistait à harmoniser les niveaux de protection au sein de l'espace communautaire pour éviter toute distorsion de concurrence et permettre la sécurisation juridique des transactions.

La pièce maîtresse de ce paquet de mesures était la proposition, devenue Directive 95/46/CE du Parlement européen et du Conseil 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. La complexité du sujet devait entraîner de longues discussions au sein du Conseil des ministres, et l'adoption des avis du Parlement européen s'étala sur une période de cinq ans. Ainsi, la directive ne fut adoptée qu'en date du 24 octobre 1995.

A ce stade, il n'était donc pas question, pour le législateur luxembourgeois, d'opérer de grands changements qui auraient été jugés prématurés et intervenant dans un cadre non encore clarifié.

I.4. Du principe de l'autorisation préalable au principe de la libre circulation

Avec le recul nécessaire qui nous est donné vingt et un ans plus tard, il y a lieu de constater que le législateur, en compagnie de nombre d'experts internationaux reconnus, avait mal prévu l'évolution de l'informatique. On relèvera toutefois le point de vue de la Chambre de commerce qui dans son avis du 12 mai 1977 critiquait déjà l'introduction d'une autorisation préalable pour le secteur privé comme *„exigence soumet(tant) les entreprises à une procédure laborieuse et irréaliste"* et aurait préféré *„un système de simple enregistrement des déclarations" (…) „à une commission indépendante"*[1] (voir document parlementaire No 2131[2], session ordinaire 1977-1978, page 4).

Cette position de la Chambre de commerce est d'autant plus pertinente qu'elle est en parfaite conformité avec le cadre communautaire actuel.

La législation de 1979 a pris le contre-pied de la position de la Chambre de commerce. Elle ne pouvait donc qu'être éloignée de l'esprit de la future Directive 95/46/CE du Parlement européen et du Conseil 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.

En effet, le principe de la libre circulation des données est reconnu dans la Directive 95/46/CE. Ceci implique nécessairement que l'on passe d'un système d'autorisation préalable à un système de plus grande liberté dans lequel l'autorisation préalable serait réduite à la portion congrue.

---

1 Ce vers quoi s'est dirigée la législation communautaire ultérieure et par conséquent le système légal en cours d'adoption devant vous.

Différents facteurs sociologiques justifient encore ce changement de système:

1) Les nouvelles technologies de la société de l'information deviennent jour après jour, le support essentiel de l'exercice des libertés d'expression et d'information et de la liberté du commerce et d'industrie.
2) La libre circulation des données est un corollaire nécessaire à la liberté du commerce et de l'industrie qui trouve aujourd'hui une application essentielle dans le développement des services de la société de l'information. Les principaux acteurs de cette société de l'information que sont les prestataires de services[1] et les destinataires de ces services attendent un cadre adapté à leurs besoins.
3) La libre circulation des données est d'autant plus importante que la dimension du Grand-Duché de Luxembourg, sa place financière exigent une facilitation et une accélération des flux de données avec un niveau de sécurité juridique accru. La spécificité de la place financière, mais aussi le nombre de sociétés y installées, ont plaidé pour l'application du projet de loi aux personnes morales comme sujet d'un traitement de données, tout du moins s'agissant des dispositions se révélant pertinentes à leur égard.

Les grandes libertés comme celle de s'établir, de s'associer ou de commercer, celle de circulation, s'appliquent aux données à caractère personnel, Ainsi, il fallait supprimer les procédures lourdes et strictes, dont l'efficacité est par ailleurs illusoire, afin de permettre l'épanouissement de ces grandes libertés dans le respect des individus.

La réforme passait donc par une refonte totale de la législation tant l'évolution technologique que celle du cadre juridique international fut importante ces 10 dernières années.

I.5. La genèse du présent projet de loi

Conscient du fait qu'il fallait avancer rapidement dans la transposition de la directive 95/46/CE afin de remédier à une situation nationale devenue totalement vétuste, le projet de loi No 4357 constituait une transposition partielle des principales dispositions de la directive 95/46; *„les dispositions de la directive nécessitant des concertations supplémentaires entre le Ministère de la Justice et d'autres instances nationales, (seraient) transposées dans un deuxième temps qui (tiendrait) nécessairement compte du délai de transposition"* à savoir 3 ans après la date d'adoption de la directive 95/46 (article 32 (2) directive 95/46) c'est-à-dire le 24 octobre 1998 (Doc. Parl. No 4357 page 15).

Par dépêche du 5 mai 1998, le président de la Chambre des Députés informa le Premier Ministre du retrait du rôle du projet de loi No 4357.

Pendant ce temps, le Ministère de la Justice était en train d'élaborer un nouveau texte portant transposition intégrale de la Directive 95/46/CE.

Le 20 septembre 1999, la Commission européenne a déposé une plainte contre le Luxembourg pour non-transposition dans le délai prescrit.

Suite au changement gouvernemental en juin 1999, la matière de la „protection des données" passait sous la compétence du Ministre délégué aux Communications. Ses services sont repris les travaux sur base des travaux préparatoires de Monsieur le Professeur POULLET tout en tenant compte des observations informelles de la Commission européenne (avis informel de la Commission du 31.1.2000) formulées au sujet d'un nouveau projet de loi élaboré par le Ministère de la Justice.

Vu l'envergure et la complexité de cette matière, l'avant-projet de loi du Ministre délégué aux Communications fut soumis à deux reprises à la consultation de tous les ministères pour qu'ils puissent faire part de leurs remarques ou recommandations.

Le projet de loi actuel est en continuité avec les travaux antérieurs et bénéficie des dernières évolutions de droit positif, doctrinales et jurisprudentielles de ces derniers mois dans le domaine de la société de l'information.

Ce projet fut réalisé par les services du Ministre délégué aux Communications et accompagné par Maître Mathieu ABBOUD, avocat-conseil.

*

1 Parmi les prestataires de la société de l'information figurent également les prestataires de services de certification soumis à la loi sur le commerce électronique du 14 août 2000 (Mémorial A No 96 du 8 septembre 2000 p. 2175) et les principes régissant la protection des données.

II. LES OBJECTIFS DU PRESENT PROJET DE LOI

II.1. Libre circulation et protection des droits des personnes

Conscient du fait que les technologies de l'information ont facilité considérablement le traitement et l'échange des données et que le volume et la rapidité des flux transfrontaliers de données ne cessent de s'accroître, les auteurs du projet de loi sous rubrique ont recherché un équilibre entre d'une part, la protection des droits et libertés fondamentaux des personnes concernées et d'autre part, la libre circulation de ces données. Cette liberté, afin de pouvoir s'exercer sans distorsion de concurrence, passe par l'harmonisation au sein de l'espace communautaire des garanties des droits et des libertés des personnes concernées par les traitements de données.

Le projet de loi repose donc sur deux piliers:

1. La libre circulation des données à caractère personnel;
2. La protection des droits et libertés fondamentaux et, en particulier, du droit à la vie privée.

Ces principes issus de la Directive 95/46/CE signifient qu'une donnée personnelle est assimilée à une marchandise[1] entrant dans le marché unique. Mais la spécificité de cette marchandise exige impérieusement qu'elle ne soit pas traitée en violation des droits et libertés fondamentaux et en particulier du droit à la vie privée.

Comme le souligne Monsieur le Professeur Frayssinet, la protection de la personne concernée englobe *les „(…) libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel. Même si partout la protection de la vie privée – notion floue et variable dans le temps et l'espace – est mise en avant, la protection va bien au-delà. Elle tend à concerner toute la vie personnelle de la personne, même la part qui n'entre pas dans le concept étroit de la vie privée (…)"*[2].

II.2. Un champ d'application précisant et dépassant celui de la directive

En vue d'instaurer un régime juridique unifié capable d'offrir un niveau de sécurité juridique approprié aux personnes concernées, le projet de loi a opté pour un champ d'application large qui s'étend également aux **personnes morales** (cf. sub 1.4.) ainsi qu'aux **personnes publiques, aux domaines de la défense, de la sécurité publique et de la sûreté de l'Etat ainsi qu'aux activités liées au droit pénal.**

L'inclusion des 4 matières susvisées (méthode adoptée par la loi portugaise et en partie par la loi belge) est permise par la Directive 95/46/CE et présente les avantages suivants:

– clarification et unification du régime juridique de la protection des données tout en autorisant à l'Etat de prévoir les limitations et dérogations nécessaires à l'exercice de la puissance publique. Certaines limitations et dérogations sont d'ores et déjà comprises dans le projet de loi. Les articles relatifs aux données sensibles, aux dérogations au droit à l'information et au droit d'accès prévoient également des dispositions limitatives et dérogatoires. Les limitations et dérogations prévues par les lois actuellement en vigueur joueront entièrement, dès lors qu'elles touchent aux personnes morales, à la défense, la sécurité publique, la sûreté et aux activités liées au droit pénal. De plus, des lois spéciales pourront à l'avenir édicter de telles limitations et dérogations.
– modifications légères des règlements grand-ducaux existants en la matière dont notamment celui du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale.

Hormis la transposition de la directive elle-même, le projet de loi contient donc certaines dispositions spécifiques.

---

1 Voilà pourquoi le projet de loi abandonne la procédure de l'„autorisation préalable" pour le plus grand nombre de traitements de données à caractère personnel, dans le secteur public comme dans le secteur privé en la remplaçant par une procédure uniforme de notification, seule garante de la libre circulation dans le respect de la vie privée et se basant sur d'autres conditions de licéité définies par la directive européenne.

2 L'Internet et la protection juridique des données personnelles par Jean FRAYSSINET Professeur à l'Université d'Aix-Marseille III intervention lors du Colloque International „L'INTERNET ET LE DROIT", Droit européen et comparé de l'internet des lundi 25 et mardi 26 septembre 2000 Grand Amphithéâtre de la Sorbonne et Sénat.

Certaines de ces dispositions spécifiques définissent un champ d'application plus large que celui de la Directive:

– l'application des dispositions de la loi touchant aux domaines de la sécurité publique, de la sûreté et des activités relatives aux domaines du droit pénal;
– l'application des dispositions de la loi aux personnes morales, dès lors qu'il s'agit de défendre leur intérêt légalement protégé.

D'autres dispositions spécifiques, plus encore qu'élargir le champ d'application, y incluent explicitement certaines hypothèse:

– l'insertion des **données génétiques dans la catégorie de traitement de catégories particulières de données (articles 6 et 7 du projet)**[1];
– **le traitement à des fins de surveillance (article 10) et plus précisément celui à des fins de surveillance sur le lieu de travail (article 11);**
– **l'interconnexion de traitements de données à caractère personnel (article 16)**[2].

Notons que sont exclus du champ d'application de la loi, les traitements de données mis en oeuvre dans le strict cadre des activités personnelles ou domestiques d'une personne physique[3]. Le comble aurait été qu'au nom de la protection de la vie privée, on entra de force dans celle des gens en exigeant d'eux des explications sur des activités menées dans le strict cadre domestique (les agendas personnels resteront donc libre d'utilisation! On pourra par exemple poser une caméra de surveillance dans son domicile si cela se fait dans le cadre et à des fins strictement domestiques).

II.3. Une loi-cadre

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

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

Ce cadre dessine l'articulation des différents textes qui interviennent sectoriellement ainsi que l'articulation des principes fondateurs de la Directive 95/46/CE avec les situations particulières exigeant des adaptations. Il s'agit donc de faire la balance des intérêts en présence.

On mentionnera pour exemple l'article 7 du projet de loi qui concerne les établissements hospitaliers mais en ne créant pas de charge importante qui risquerait d'en freiner le fonctionnement. Ainsi, l'articulation des textes s'est faite dans le souci de préserver le fonctionnement des services hospitaliers tout en respectant les grands principes de la protection des données.

Pour exemple encore, l'articulation avec la loi relative au commerce électronique (…) issue du texte même de cette loi[4]. L'article 2 paragraphe (3) de la loi relative au commerce électronique (…) dispose que *„les dispositions de la présente loi s'appliquent sans préjudice des dispositions relatives à la protection des données personnelles.“*.

---

1 Les données génétiques ne sont pas explicitement visées par la directive 95/46/CE. Elles entrent pourtant parfaitement dans la définition de la donnée à caractère personnel.

2 Le considérant 53 de la directive 95/46/CE souligne qu'il est nécessaire de soumettre à autorisation préalable „certains traitements susceptibles de présenter des risques particuliers au regard (…) de leurs finalités (…) ou du fait de l'usage particulier d'une technologie nouvelle. Il vise, ce faisant, indirectement l'hypothèse de l'interconnexion.

3 Juridiquement les activités personnelles ou domestiques des personnes privées sont hors du champ du projet de loi.

4 en amont l'articulation est issue de textes communautaires comme la directive 1999/93 relative à un cadre communautaire pour les signatures électroniques spécialement pour le service de certification.

Cette articulation est encore précisée à l'article 20 paragraphe (1) de la loi sur le commerce électronique (…) s'agissant plus particulièrement des prestataires de service de certification:

„(1) L'Autorité Nationale d'Accréditation et de Surveillance et les prestataires de service de certification sont tenus au respect des dispositions légales régissant le traitement de données à caractère personnel (…)."[1].

Ce système permet de façon transparente de tracer le cadre général de la protection des droits et libertés fondamentaux de la personne concernée, tout en composant avec des principes tels que la libre circulation, la libre prestation, l'intérêt public... Ainsi, cette balance d'intérêts ne compromet jamais la protection des droits et libertés fondamentaux qui restent au centre des questions, tout en admettant les adaptations nécessaires. Pour exemple, les règles spéciales relatives à la légitimation de la collecte de données personnelles par des prestataires de certification et prévues dans le loi relative au commerce électronique sont en parfaite conformité avec la lettre et l'esprit de la Directive 95/46/CE.

L'édiction des règlements grand-ducaux permettra de parfaire l'édifice en précisant certaines règles pour la bonne application de la loi.

Certains règlements sont à prendre impérativement, d'autres interviendront facultativement.

b) *La liste des règlements grand-ducaux (RGD ci-après)*

1. RGD relatif à la mise en oeuvre de traitements de données à caractère personnel par le corps de police
   – base légale primaire: article 17 texte de loi
   – base légale secondaire: article 3 (5) texte de loi
   – il s'agit d'une reprise et d'une mise à jour du RGD du 2 octobre 1992 abrogé de facto suite à l'abrogation de la loi du 31 mars 1979 (article 44 du projet de loi)
2. RGD relatif à la mise en oeuvre de traitements de catégories particulières de données par les services de la santé
   – base légale: article 7 (4) texte de loi
3. RGD fixant le montant et les modalités de paiement d'une redevance à percevoir dans le cadre de la procédure de notification
   – base légale: article 13 (5) texte de loi
4. RGD relatif aux modalités d'exercice de la fonction du chargé de la protection des données
   – base légale: article 40 (10) texte loi
5. RGD déterminant la nature, le format et les modalités de mise à dispositions des données des abonnés des opérateurs de télécommunications et/ou des services postaux et/ou de leurs fournisseurs de services dans le cadre de l'article 41 (1)
   – base légale: article 41 (1) texte de loi
6. RGD fixant le cadre du personnel de la Commission nationale pour la protection des données
   – base légale: article 38 (2) texte de loi
7. *possibilité* d'un RGD déterminant les modalités de mise en oeuvre des traitements faisant l'objet d'une interconnexion
   – base légale: article 16 (3) texte de loi
8. *possibilité* d'un RGD pouvant ajouter à la liste des professions réglementées d'autres catégories de personnes pouvant exercer la fonction de chargé de la protection des données
   – base légale: article 40 (8) texte de loi
9. *possibilité* d'un RGD déterminant les modalités de la procédure contradictoire
   – base légale: article 35 (3) texte de loi

1 Ainsi, les certificateurs sont soumis aux règles de la protection des données et l'article 20 paragraphes (2) et (3) de la loi relative au commerce électronique (…) fait une application sectorielle de ce principe. Cette application est en parfaite conformité avec la loi sur la protection des données.

Remarque: il est envisagé de transposer par RGD la directive 97/66/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications

– bases légales: loi sur la protection des données
  loi du 21 mars 1997 sur les télécommunications

Les règlements grand-ducaux obligatoires sont élaborés dès à présent pour pouvoir en principe être publiés ensembles, avec la loi.

II.4. L'importance du projet de loi pour la protection des droits et libertés fondamentaux, et en particulier de la vie privée

L'ensemble des droits des personnes, qu'ils soient réels ou personnels, se rattachent d'une manière ou d'une autre à l'identité de leur titulaire, de sorte que l'ensemble de la vie sociale ou privée d'une personne constitue un spectre se rattachant à elle.

En ce sens, toute activité humaine peut être répertoriée comme une donnée personnelle. Bien entendu, toute activité n'est pas digne d'inventaire, ni susceptible de présenter un danger pour la personne qui la mène.

Le risque d'atteinte à la vie privée et aux droits et libertés fondamentaux de la personne concernée est fonction de la nature de la donnée, des moyens de collecte et surtout de la finalité de cette collecte. Le risque est naturellement accru par l'émergence des nouvelles technologies.

Ce risque existe vis-à-vis de la puissance publique comme du secteur privé. En effet, sans négliger le risque de surveillance étatique des administrés[1], les moyens de cette surveillance sont à la portée du plus grand nombre. En effet, la surveillance des postes informatisés de travail[2] de même que la surveillance de la navigation sur Internet (programmes cookies) par l'utilisation de programmes, lesquels permettent à tous et pour peu de frais d'avoir accès à des technologies avancées.

La navigation sur Internet elle-même et indépendamment de tout acte d'adhésion ou de tout comportement actif sur la toile peut constituer un ensemble de données personnelles stratégiques. En effet, savoir sur quel site est allé l'internaute revient à connaître ses goûts de consommateur, mais aussi éventuellement son appartenance politique ou ses pratiques sexuelles et *„l'internaute, de manière directe ou indirecte, visible ou invisible, volontaire ou involontaire livre, comme le Petit Poucet semait des petits cailloux, des données directement ou indirectement personnelles ou des traces, qui donnent lieu à un fichage traditionnel ou à des traitements complexes souvent nécessaires pour satisfaire ses propres intérêts mais aussi utilisables à son insu et défavorablement.“*[3].

On comprend dès lors l'importance de l'édiction d'une législation protectrice des droits et libertés fondamentaux et en particulier de la vie privée au regard de l'utilisation de toutes les données se rattachant à un individu ou à une personne morale.

La grande variété des hypothèses est fonction de l'identité de la personne qui collecte, des besoins de celle-ci, de la finalité de la collecte et de la nature des données collectées. Ceci a conduit, les auteurs du projet de loi à adopter une approche casuistique, combinant l'application des principes et leurs dérogations. Ainsi, de nombreuses hypothèses sont étudiées et de nombreux cas analysés. Ce texte regorge de solutions diverses qui elles-mêmes renvoient à des mécanismes de droit matériel et à des procédures variées[4].

---

1 Les discussions du Parlement européen au sujet d'Echelon, système de surveillance planétaire mis au service des Etats-Unis et des Etats du Commonwealth et de la riposte européenne rappelle que big brother n'est pas tout à fait mort.

2 Cette question fait naître une jurisprudence en droit du travail chez nos voisins français. i.e.: le tribunal correctionnel de Paris a, le 2 novembre 2000, dans une affaire 9725223011, jugé que „les e-mails“ sur le lieu de travail étaient couverts par le secret de la correspondance.

3 Intervention de Monsieur le Professeur FRAYSSINET op. cit. No 10.

4 Le projet de loi, tout en reprenant le plus souvent et sous forme abrégée les règles applicables procède également par renvoi. Cette solution a trois avantages:

– elle permet au praticien de retrouver rapidement la règle applicable à une hypothèse bien définie;

– elle permet d'élaborer (en cours) une version avec hyperliens ce qui, pour une matière en relation avec les nouvelles technologies semble être une contribution adéquate au droit et en faveur de ses utilisateurs;

– elle permet d'éviter, s'agissant d'une matière déjà complexe, les lourdeurs textuelles inutiles et constituées par de nombreuses répétitions exhaustives des règles à appliquer. Ainsi, le lecteur habituel du texte et l'utilisateur de l'outil informatique retrouveront un texte sous forme de parcours fléché, dans le dédale complexe et sensible de la protection des données.

A travers ce texte protecteur un fil conducteur se dégage; il s'agit du „principe de finalité" du traitement. C'est par la finalité du traitement que tout commence et tout finit.

En effet, la finalité:

– doit être antérieure à la mise en oeuvre du traitement;
– justifie la collecte;
– doit être connue de la personne concernée;
– limite le champ de l'utilisation des données collectées;
– une fois réalisée exige que les données collectées soient détruites (durée de conservation)[1].

Ce principe de finalité est le seul à ne pouvoir être dépassé par la technologie car il s'exerce sur l'homme qui l'utilise.

II.5. Une loi importante pour le développement du monde économique

a) *Un complément indispensable à la loi relative au commerce électronique et aux besoins du commerce électronique*

Le développement actuel du commerce électronique est freiné (les questions relatives à la sécurisation du paiement, à l'identification claire du cocontractant apparaissent souvent) par la sensation d'insécurité juridique des différents opérateurs économiques, qu'ils soient consommateurs ou commerçants.

Le cas du consommateur naviguant sur Internet est particulièrement révélateur. Ce secteur, connaît un essor moins grand et c'est autour du consommateur „naviguant" que se concentrent toutes les inquiétudes. Le consommateur se demande qui est son interlocuteur, auprès de qui pourra-t-il se plaindre en cas de problème, comment être sûr que le paiement qu'il effectue est sécurisé et s'il ne risque pas d'être englouti dans des systèmes l'analysant et le calibrant à chacun de ses mouvements.

La loi sur le commerce électronique règle d'ores et déjà un grand nombre de questions, comme celles relatives à la sécurisation des paiements, l'identification du cocontractant, mais, restent toujours les questions relatives à l'utilisation des données personnelles.

C'est ici que la protection des données personnelles, vient compléter le dispositif de sécurisation juridique, pour permettre le développement de l'utilisation de la toile et plus particulièrement du commerce électronique.

Ainsi, les réglementations relatives au commerce électronique, à la protection des données personnelles sont les pans d'une même toiture sous laquelle l'individu consommateur s'abritera et consommera librement en toute sécurité.

b) *La place financière*

Le e-commerce se développe dans tous les secteurs de l'économie et l'émergence tant au niveau international que local du e-banking ne fait plus de doute.

Il faut que soient respectés les intérêts des Professionnels du Secteur Financier (PSF ci-après), les droits et libertés fondamentaux du client en tant que sujet d'un traitement de données le concernant, le principe de la libre circulation ainsi que celui de la libre prestation au sein de l'Union européenne.

A ce stade, on peut se demander si les obligations incluses dans la réglementation sur la protection des données sont compatibles avec celles auxquelles sont assujetties les PSF.

L'article 41 de la loi modifiée du 5 avril 1993 relative au secteur financier est parfaitement compatible avec les exigences découlant des droits et libertés de la personne concernée, qui en l'occurrence, est le client du PSF. En effet, le client du PSF ne veut voir traiter des données le concernant que dans le cadre bien finalisé du contrat le liant au PSF, sans qu'aucune communication vers l'extérieur et hors du champ du contrat ne soit permise. Ainsi, il existe une réelle convergence d'intérêts entre les différentes législations.

---

1 Un parallèle peut-être fait avec l'objet social d'une entreprise, celui-ci est défini à la constitution et l'entreprise ne pourra pas exercer d'activité dépassant son objet social sans avoir à modifier l'acte constitutif.

L'expression finale de cette convergence est la réaffirmation des obligations auxquelles, les PSF sont assujettis et en particulier, celle de l'article 41 de la loi modifiée du 5 avril 1993 relative au secteur financier. La responsabilité des PSF est de développer des systèmes respectueux de cette contrainte.

Le développement de tels systèmes nécessitera probablement une concertation entre les PSF.

Il faudra par exemple, aménager l'intervention du prestataire de service de certification qui est un des piliers du développement du e-banking. Cet aménagement devra se faire en respectant les principes de libre prestation de service et de libre circulation des données.

Là encore, le projet de loi sur la protection des données converge et offre des outils à une telle concertation à travers la corégulation. En effet, le projet de loi prévoit un tel mécanisme sous le nom de „code de conduite".

Le code de conduite est un document sectoriel, rédigé entre les représentants du secteur concerné et afin de permettre une application meilleure et adaptée de la loi sur la protection des données. Le code de conduite pourrait ici exprimer la convergence entre les objectifs de la loi relative au secteur financier et ceux de la loi relative à la protection des données. Cette convergence une fois réaffirmée pourrait être accompagnée de différents modus operandi à mettre en oeuvre, ainsi que de contrats types à utiliser.

Le code de conduite pourra être négocié au niveau national ou communautaire, approuvé ou non par la Commission nationale pour la protection des données. Une telle approbation, si elle est facultative, ne ferait que renforcer la légitimité d'un tel document.

Ce code de conduite pourrait également tracer les lignes directrices de la mise en place en concertation avec la place financière d'un „data center" au Grand-Duché de Luxembourg qui, outre l'aspect strictement économique, pourrait résoudre une partie des problèmes vus ci-dessus.

Ce document pourrait enfin avoir un rôle déterminant dans l'explication des enjeux, et ceci dans l'intérêt de la place financière, et pourrait être rédigé en collaboration avec d'autres autorités comme la Commission de Surveillance du Secteur Financier.

II.6. Une loi devant améliorer l'utilisation des banques de données publiques

Le secteur public est soumis à la loi. Toutefois, il faut lui permettre de continuer à améliorer sa gestion dans l'intérêt de la collectivité.

La loi, tout en soumettant le secteur public devra donc:

a) ne pas paralyser le fonctionnement des administrations publiques et permettre des améliorations au fonctionnement des services;

b) ne pas entraver l'activité régulière de l'administration;

c) tenir compte des impératifs liés à la puissance publique et plus précisément aux nécessités liées à la sécurité publique, la défense, la sûreté et les activités de l'Etat relatives à des domaines du droit pénal.

Ces trois impératifs seront respectés sans porter atteinte aux droits et libertés fondamentaux, dont le droit à la vie privée de la personne concernée.

a) *L'amélioration du fonctionnement des administrations publiques*

Pour éviter la paralysie des administrations publiques, le projet de loi prévoit certaines dérogations à l'obligation d'informer la personne concernée de la mise en oeuvre de tout traitement de données personnelles la concernant. Ce sont les cas, qui auraient générés une surcharge de travail disproportionnée au regard des enjeux pour la personne concernée et des contraintes de fonctionnement de l'administration. Par exemple, l'utilisation des données de l'état civil d'une personne, afin d'ouvrir un dossier pour l'attribution d'un droit par un organisme de sécurité sociale, n'exigera a priori pas l'information de la personne concernée. En effet d'une part le droit attribué le sera au bénéfice de la personne concernée et d'autre part, les données traitées ne sont pas a priori, susceptibles d'atteinte à ses droits fondamentaux. Dès lors, l'information de la personne concernée sera a priori facultative, afin de permettre le bon fonctionnement du service. Toutefois, il ne saurait être question d'utiliser abusivement cette exemption à certaines charges de la loi. En toute hypothèse, la loyauté des administrations publiques sera contrôlée par la Commission nationale pour la Protection des données (ci-après „la

Commission“) et le cas échéant par le juge administratif qui pourra qualifier un détournement de procédure.

Par ailleurs, une amélioration majeure et nécessaire au fonctionnement des administrations publiques a été apportée. En effet, celles-ci pourront dorénavant et sous certaines conditions interconnecter leurs différents fichiers. Cette possibilité était écartée sous l'ancien régime.

b) *La préservation de l'activité régulière de l'administration*

L'article 5 paragraphe (1) (b) de la loi prévoit que le traitement de données peut être effectué si *„(…) le* ***traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique****, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées (…)“*. Ainsi, l'activité de l'administration est entièrement préservée. Celle-ci pourra collecter et traiter des données relatives à ses administrés afin de remplir sa mission.

L'administration devra toutefois respecter le droit d'opposition de l'article 30 paragraphe (1) du projet de loi. Cet article permet à la personne concernée ***„(…) 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 (…)“.*** Il s'agit ici de faire la balance entre la mission de l'administration et la situation particulière de l'administré. En tout état de cause, un administré ne pourra pas brandir l'article 30 paragraphe (1), face à l'agent public qui l'interpelle. Il faudra qu'il justifie de sa situation particulière. En cas de litige c'est la Commission nationale pour la protection des données qui arbitrera. De plus, la situation particulière de l'administré ne pourra, bien entendu, pas être soulevée, si c'est la loi qui prévoit expressément la collecte de données[1] par l'agent public.

Cette balance est respectueuse des droits de la personne concernée tout en préservant le principe de continuité de l'Etat et de ses missions.

c) *Les impératifs liés à la puissance publique*

Enfin, il a été tenu compte des impératifs liés à la puissance publique et plus précisément aux nécessités liées à la sécurité publique, la défense, la sûreté et les activités de l'Etat relatives à des domaines du droit pénal. En effet, le domaine judiciaire est entièrement préservé, quant aux autres domaines, ils restent sous le contrôle de l'exécutif conformément à l'article 17.

*

III. RESUME DES PRINCIPALES DISPOSITIONS DE LA LOI

III. 1. La donnée

a) *La définition (article 2 (a))*

Une donnée à caractère personnel peut être toute information relative à une personne qui est identifiée ou qui est identifiable („personne concernée“). Les données codées mais décodables par un intermédiaire quelconque sont des données personnelles.

La principale nouveauté est qu'une donnée est personnelle, indépendamment de son support ou de sa forme. En effet, la notion d'information n'est pas définie. Dès lors, elle n'est soumise à aucune exigence de forme particulière. On souligne donc, reprenant en cela le considérant (14) de la Directive, *„que, compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives aux personnes (…)“* sont des données à caractère personnel entrant dans le champ de la loi.

---

1 On rappelle ici, qu'une collecte de données constitue un traitement et donc, qu'une loi prévoyant expressément cette collecte par l'agent public dans le cadre de ses missions, remplira la condition de l'article 30 paragraphe (1) in fine.

Le considérant (26) de la Directive 95/46/CE précise *„que, pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en oeuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne"*.

b) *Les caractéristiques de qualité du traitement des données (article 4 de la loi)*

Les principes permettant de garantir une qualité élevée lors du traitement de données sont:

– la loyauté qui interdit au responsable du traitement d'agir à l'insu de la personne concernée;
– la finalité explicite et légitime qui est le fil conducteur du responsable du traitement. Il ne peut s'en écarter et ceci dans l'intérêt de la personne concernée;
– l'adéquation, la pertinence, l'exactitude, la mise à jour et la durée de conservation des données limitée à ce qui est nécessaire au traitement, à savoir le temps nécessaire pour atteindre sa finalité. Ces principes ne sont que des prolongements des principes de loyauté et de finalité.

III. 2. *Le traitement*

a) *Définition (article 2 (c))*

Le traitement de données à caractère personnel est la notion qui se substitue à celle de banque de données. L'évolution technologique exigeait cette évolution terminologique. En effet, la notion de banque de données se rapporte à un phénomène centralisé et localisé. Or, on sait que les données ne sont plus stockées et utilisées en un seul lieu mais que la tendance la plus forte est à la décentralisation, à la dispersion des données qui sont rassemblées par le responsable du traitement, à une fin et en un instant par le biais du réseau Internet.

La loi s'applique aussi bien à un traitement automatisé que non automatisé de données à caractère personnel, contenues ou appelées à figurer dans un fichier tel que défini à l'article 2 sous (d). Cette définition est très large. Ainsi, quasiment toute forme de traitement sera soumise à la loi, même le traitement le plus simple et le plus isolé. Ceci est nécessaire, du fait du développement des nouvelles technologies qui permettent, à partir de données personnelles parcellaires et totalement décentralisées, de recomposer un ensemble complexe autour de personnes identifiées ou identifiables, ceci par le biais des moteurs de recherche.

b) *Les traitements exclus: les activités personnelles ou domestiques (article 3 paragraphe 3))*

L'activité domestique d'une personne physique n'entre pas dans le champ d'application du projet de loi et un traitement de données, mis en oeuvre dans ce cadre, est totalement libre. Il aurait été paradoxal d'édicter des régies protectrices de la vie privée, qui auraient envahi elles-mêmes, la sphère privée de la vie de chacun. On aurait atteint un résultat contraire au but assigné à la protection des droits et libertés fondamentaux et ainsi violé l'esprit de la loi. Si l'on n'avait pas prévu cette exclusion du champ d'application, l'arbre de la justice aurait assombri un peu plus encore le ciel des libertés individuelles.

Ajoutons bien entendu que les personnes morales ne peuvent revendiquer d'activités personnelles ou domestiques propres, elles ne pourront dès lors échapper à la loi sur cette base.

c) *La légitimité de la personne mettant en oeuvre un traitement (article 5)*

La légitimité est ce qui fonde un responsable de traitement à agir en tant que tel. Ainsi, pour pouvoir collecter des données personnelles, il faut pouvoir se fonder sur une des hypothèses de légitimation de son action telles qu'énumérées à l'article 5.

Parmi elles, il y a le consentement exprès de la personne concernée. Ce consentement, s'il est éclairé, est un passe-partout.

A côté de ce passe-partout, d'autres clefs n'ouvrent qu'une porte permettant les traitements de données de façon limitative:

– afin de respecter une obligation légale,
– si le traitement est nécessaire pour une mission d'intérêt public ou relevant de l'exercice de l'autorité publique (sont visés ici les réquisitions de l'autorité publique, les services de santé intervenant d'urgence pour sauver la vie des tiers …),
– pour l'exécution d'un contrat ou de mesures précontractuelles demandées par la personne concernée,
– pour les nécessités de la réalisation de l'intérêt légitime poursuivi par le responsable du traitement (son objet social s'il s'agit d'une personne morale),
– pour la sauvegarde de l'intérêt vital de la personne concernée.

d) *Les conditions de mise en oeuvre d'un traitement*

Une fois énumérées, les obligations positives que doit respecter la personne qui traite des données (finalité, loyauté …) et les hypothèses de légitimation d'un tel traitement, il faut définir les modalités et les contraintes auxquelles le traitement à mettre en oeuvre est soumis. En effet, la légitimité qu'un responsable de traitement peut avoir à traiter des données à caractère personnel, ne doit pas l'autoriser à faire en pratique tout et n'importe quoi.

– la confidentialité (article 21)

L'article 21 précise que toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter, sauf en vertu d'obligations légales[1], que sur instruction du responsable du traitement.

La confidentialité se base ici sur la limitation des intervenants et sur l'exigence d'un ordre émanant du responsable du traitement.

La confidentialité est ainsi garantie, alors que la manipulation des données se fait seulement sur autorisation du responsable du traitement, ce qui limite au minimum la diffusion des données.

– la sécurité (articles 22 et 23)

La sécurité doit être garantie, car à quoi bon responsabiliser fortement le responsable du traitement dans ses rapports avec les tiers (sous-traitants …) si le système, le plus souvent informatique, n'offre pas une sécurité en termes d'objectifs et de spécificités techniques.

Ainsi, lorsque des données sont traitées, un certain nombre d'objectifs, qui se traduiront par la mise en place d'une pratique de la sécurité, permettront de se prévenir contre les „fuites" de données, les détournements et autres pertes de données.

Ces objectifs sont énumérés de façon générale dans l'article 22 et sont précisés en termes plus opérationnels dans l'article 23.

Au stade actuel, les données ont été collectées licitement c'est-à-dire dans de bonnes conditions qualitatives, légitimement, dans une stricte confidentialité garantie par une sécurisation du système de traitement des données quel qu'il soit. Il faut alors analyser quels sont les droits de la personne, droits positifs lui permettant de garder le contrôle de bout en bout de la chaîne du traitement des données.

e) *Les droits de la personne concernée*

Ces droits ont pour principal but, le maintien de la transparence lors des opérations de traitement des données à caractère personnel. Cette transparence est nécessaire pour permettre à la personne concernée, de vérifier que le responsable du traitement reste dans la droite ligne de la loi et le cas échéant, en cas d'abus, pour permettre à la personne concernée de faire valoir et de réintégrer ses droits et libertés fondamentaux.

– le droit à l'information (articles 26 et 27)

Ce droit à l'information est en fait une obligation d'information à charge du responsable du traitement. La personne concernée devra toujours être informée de façon à pouvoir identifier, d'une part, le responsable du traitement et le cas échéant son représentant d'autre part, le traitement lui-même et les

1 Il peut s'agir, par exemple, des dispositions de la législation en matière de blanchiment d'argent.

droits dont elle bénéficie. Cette information se fera au plus tard au moment de la collecte originelle, qu'elle ait eu lieu ou non directement auprès de la personne concernée, ou encore lorsqu'est envisagée la première communication de données à un tiers.

Ces règles s'appliquent aussi bien s'il s'agit d'une collecte „intuitu personae" que lors d'une collecte par la voie d'un formulaire type. Tout au long de la vie de la donnée, la personne concernée devra être tenue informée. Toutefois, la loi prévoit des exceptions à ce droit d'information.

De telles exceptions existent dans les domaines de la sécurité publique, de la sûreté de l'Etat, de la défense, de même que lors du traitement de données effectué dans le cadre de la protection de la personne elle-même (urgence par exemple) ou de la protection des droits et libertés d'autrui, le droit à l'information disparaît. De même, afin de protéger la liberté d'expression, le droit des artistes et des journalistes, l'obligation d'information est réduite. A cette fin, la protection de la collecte des informations par le journaliste est garantie.

L'exception la plus importante exempte de l'obligation d'information, lorsqu'elle impliquerait un effort disproportionné (ex. traitement ayant une finalité statistique, historique, scientifique). Il s'agit de garantir le bon fonctionnement du secteur public et du secteur privé en leur évitant une surcharge qui les paralyserait. Toutefois, cette exception ne devra pas permettre la violation des principes de finalité et de loyauté, qui restent au coeur du dispositif juridique.

Enfin, l'hypothèse de l'autorisation de la loi à enregistrer et communiquer des données est également exonératoire de l'obligation d'informer.

– le droit d'accès (articles 28 et 29)

Le deuxième droit fondamental de toute personne est d'avoir accès aux données la concernant. Ce droit comporte différentes facettes:

* le droit d'obtenir la confirmation de l'existence d'un traitement, de même que les données traitées au sujet de la personne concernée, y compris la communication de ces données sous une forme intelligible;
* le droit de rectification, d'effacement ou de verrouillage des données dont le traitement n'est pas conforme à la présente loi, ainsi que
* le droit de disposer d'un recours.

Il est fondamental que ce droit soit garanti et qu'il puisse s'exercer sans contrainte et sans frais.

Si lors de l'exercice de son droit d'accès, la personne concernée a de sérieux doutes quant à la conformité des données communiquées par le responsable du traitement, ceci par rapport à celles qui seraient effectivement traitées, elle peut se tourner vers la Commission nationale pour la protection des données qui agira dans le cadre des pouvoirs qui lui sont conférés.

Les données collectées par un médecin doivent être soumises au droit d'accès. Il s'agit d'une application en parfaite conformité avec l'article 36 de la loi du 28 août 1998 sur les établissements hospitaliers.

L'article 29 prévoit les raisons pour lesquelles l'exercice du droit d'accès peut être refusé, limité ou différé par le responsable du traitement. Les exceptions au droit d'accès sont, en dehors des attributs de la puissance publique (sûreté, sécurité, activités pénales …), la protection de la personne concernée ou des droits et libertés d'autrui, ainsi que le cas dans lequel *„… il n'existe manifestement aucun risque d'atteinte à la vie privée d'une personne concernée, … lorsque les données sont traitées exclusivement aux fins de recherche scientifique ou sont stockées sous la forme de données à la seule finalité d'établissement de statistiques …"*.

Le droit d'accès s'articule de façon particulière avec la liberté d'expression. Il n'est qu'indirect et cette limitation en fait une exception au droit d'accès classique. L'exercice de ce droit peut mettre en danger la finalité du traitement (cf. infra III.3. D La liberté d'expression).

– le droit d'opposition (article 30)

Le droit d'opposition est un droit nouveau. Il est inconditionnel dès lors que la finalité du traitement est la prospection qu'elle soit commerciale, politique, associative (etc). Ainsi, le droit d'opposition relatif aux publicités non sollicitées pourra être soulevé sans aucune discussion.

Le droit d'opposition est également inconditionnel pour les décisions individuelles automatisées. On sait celles-ci prohibées pour les décisions administratives individuelles (principe de l'examen particu-

lier de chaque demande), la question se posera donc principalement pour le secteur privé. L'hypothèse la plus fréquente concerne le credit-scoring et l'évaluation du personnel. De telles décisions individualisées conditionnent l'octroi d'un droit, et à ce titre appellent le jeu inconditionnel du droit d'opposition.

Dans tous les autres cas, le droit d'opposition ne sera possible que si, en présence d'un traitement légitime, des raisons prépondérantes et légitimes tenant à la situation particulière de la personne concernée existent.

– le droit de ne pas être soumis à une décision automatisée (article 31)

C'est un corollaire du droit d'opposition. Cet article transpose l'article 15 de la directive 95/46/CE sur les décisions individuelles automatisées. Il instaure un droit de ne pas être soumis à une telle décision. Ce droit est inconditionnel. Les principales applications de ce type particulier de décisions concernent essentiellement le credit-scoring et l'évaluation du personnel.

A ce stade, nous avons dessiné les contours du droit commun de la protection des données. Certaines catégories de traitements sont particulières et de cette particularité naît un ensemble de régimes spéciaux plus ou moins dérogatoires au droit commun.

III. 3. Les catégories particulières de traitements

Les catégories particulières de traitement les plus importantes sont celles relatives aux catégories particulières de données dites encore données sensibles.

A. *Le traitement de catégories particulières de données dites encore données sensibles*

a) *Principe de l'interdiction*

Le projet de loi reprend de la directive 95/46, le **principe de l'interdiction du traitement de catégories particulières de données à caractère personnel dites „données sensibles“** (article 8 de la directive). Il s'agit des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé et à la vie sexuelle. On y a ajouté les données génétiques. Cet ajout est opportun, alors que le traitement de données génétiques est de plus en plus fréquent, tant dans le domaine de la santé, que dans celui des assurances et de l'emploi.

b) *Les exceptions générales au principe (l'article 6 paragraphe (2))*

Contrairement à la loi du 31 mars 1979, qui ne prévoyait aucune exception au principe de l'interdiction du traitement de données à caractère personnel sensibles, la Directive 95/46/CE fixe, de manière détaillée, les règles matérielles légitimant le traitement de telles données.

– les exceptions soutenues par le consentement de la personne concernée

S'agissant des données dites sensibles, le consentement exprès de la personne concernée peut légitimer un traitement. Ce consentement ne sera toutefois pas un passe-partout universel.

Ainsi, le consentement exprès à un tel traitement ne légitime le traitement que s'il ne s'oppose pas au principe de l'indisponibilité du corps humain et sauf le cas où la loi prévoit que l'interdiction ne peut être levée par le consentement de la personne concernée. On fait donc référence à la loi et à l'indisponibilité du corps humain comme limite au consentement.

La mention de l'indisponibilité du corps humain, si elle véhicule son lot d'incertitudes, appréhende certains comportements déviants tels l'eugénisme ou la reproduction cellulaire aboutissant au clonage, dans une matière où donnée et support organique ne sont pas obligatoirement dissociés et alors que la récolte de données peut aboutir à des abus par l'utilisation des technologies de biologie appliquée.

Cette disposition permet de réserver l'avenir et d'inclure des hypothèses scientifiques non encore connues. De manière plus générale, l'évolution de la matière du traitement des données poussera probablement le législateur à intervenir à nouveau en cas de besoin.

Le consentement de la personne concernée légitimera particulièrement le traitement effectué dans le cadre des activités de la vie associative à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux données nécessaires et relatives aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité.

Entre la légitimation sur base du consentement et d'autres hypothèses spéciales se trouve le traitement de données rendues publiques par la personne concernée (il serait certainement vain de demander à un homme politique de donner son consentement explicite pour que l'on puisse „révéler" qu'il appartient à tel ou tel parti politique). En effet, on peut admettre, que le fait de rendre public de telles données est une forme de consentement de la part de la personne concernée. Un tel consentement implicite aurait probablement été insuffisant à lui seul mais, supporté par la nature publique des données, il est soutenu à suffisance et légitime le traitement.

– *les exceptions indépendantes du consentement de la personne concernée*

Il existe d'autres cas où il est nécessaire et légitime de traiter des données à caractère personnel dites sensibles et dans lesquels il n'est pas toujours possible, ni par ailleurs opportun, de requérir le consentement de la personne concernée par le traitement.

Il en sera ainsi, dans les domaines:

– des obligations du droit du travail (cette hypothèse est reprise in extenso du texte de la directive et est sans application actuelle au Grand-Duché de Luxembourg),
– de la sauvegarde de la vie (ex.: traitement dans un cas d'urgence médicale, la personne concernée se trouve dans le coma et il y a lieu de procéder à une greffe d'organe qui exige certaines analyses de données médicales à caractère personnel du patient et/ou du donneur),
– des traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice,
– de l'intérêt public important (ex. de façon non exhaustive sont de tels motifs les traitements mis en oeuvre à des fins historiques, statistiques ou scientifiques),
– de la prévention, à la recherche, à la constatation et à la poursuite des infractions pénales et les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique (s'ils connaissent un régime spécifique, ils font évidemment partie des motifs d'intérêt public important et sont visés par renvoi à l'article 17).

c) *Les procédures judiciaires: les besoins de la bonne administration de la justice*

Cette exception à la prohibition de traiter des données dites sensibles est tirée de la nature de la procédure en cause. La justice fonctionne dans le cadre du contradictoire et autour du principe du respect des droits de la défense. Ces principes assurent l'information de la personne concernée. Ils sont autant de garanties conformément au principe de loyauté et de finalité. On ne saurait donc imposer une quelconque prohibition générale à la justice.

Toutefois, le projet de loi prévoit une limitation relative aux données génétiques. Celles-ci ne peuvent être traitées que dans le cadre de l'administration de la preuve, pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée. Ces limites sont reprises de la recommandation R97/5 du Conseil de l'Europe et sont conformes au bon fonctionnement de la justice.

d) *Les données génétiques (article 6 paragraphes (3) et (4) et article 7)*

Tout d'abord il ya lieu de rappeler que toute donnée génétique quel que soit son caractère scientifique n'est pas nécessairement relative à la santé. Par exemple, le gène récessif ou dominant déterminant la couleur des cheveux ou celui déterminant leur nombre ne pourra pas a priori être classé dans la catégorie des données relatives à la santé de la personne concernée. Ceci justifie la distinction entre ces notions tant au niveau des définitions que dans la structure des articles 6 et 7 de la loi.

L'optique est ici, de restreindre encore les cas permettant le traitement de données génétiques par rapport aux hypothèses des données dites sensibles en général. Il s'agit ici de permettre l'expérimentation, le développement de la technique et de la science tout en se dotant de gardes fous indispensables.

La restriction consiste à ne permettre le traitement des données génétiques que pour certains des cas prévus dans le cadre des exceptions générales à l'interdiction de traiter des données sensibles (cf. b).

Ainsi, le régime des données génétiques est encore plus restrictif que celui des catégories particulières de données, dites données sensibles dans la mesure où le traitement de données génétiques n'est possible que dans certains cas.

Le projet de loi vise les hypothèses dans lesquelles il est manifestement nécessaire de pouvoir traiter des données génétiques:

– lorsque le traitement est nécessaire à la sauvegarde de la vie de la personne concernée ou d'une autre personne, dans le cas où la personne concernée se trouverait dans l'incapacité physique ou juridique de donner son consentement;
– lorsque le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice;
– dans le cadre de la réalisation de motifs d'intérêts publics importants, comme ceux de la recherche scientifique, historique, des statistiques publiques;
– dans les hypothèses visées à l'article 17 de la loi (nécessité pour la défense, la sûreté de la sécurité publique, activité pénale);
– dans le cadre des procédures judiciaires avec les limites vues ci-dessus (cf. c));

Il appartiendra au législateur d'intervenir à nouveau en fonction des évolutions de la société et de l'état de la science.

L'hypothèse du consentement de la personne concernée est traitée de façon particulière et constitue une limitation de la loi. Cette limitation est préconisée dans le rapport de Monsieur Guy BRAIBANT (op. cit.). Le consentement de la personne concernée ne pourra justifier un traitement de données génétiques que si ce traitement a pour finalité la santé ou la recherche scientifique. Il s'agit ici, d'une application particulière de la prohibition de la loi. Cette prohibition de la loi prend la forme d'une limitation. Il ne s'agit pas de prohiber totalement car il faut permettre la recherche pour améliorer l'état de nos connaissances tout en limitant par ailleurs le traitement à la seule fin de la santé de la personne concernée. Notons que la réserve générale de l'indisponibilité du corps humain couvre également ce cas de figure.

B. *Le traitement de catégories particulières de données par les services de la santé (article 7)*

On définit les conditions de traitement des catégories particulières de données par les services de la santé. On a défini un régime propre à la finalité qu'est la santé et plus largement la santé publique. Ainsi, on vise plus particulièrement les données relatives à la santé, sans exclure les autres catégories de données dites sensibles.

a) *Les cas d'ouverture*

Le traitement est licite, lorsque le traitement de catégories particulières de données est nécessaire:

– aux fins de la médecine préventive,
– aux diagnostics médicaux,
– à l'administration de soins ou de traitements médicaux,
– à la recherche scientifique dans le domaine de la biologie et de la médecine,
– à la gestion de services de santé.

b) *Les personnes autorisées*

Ces traitements pourront être mis en oeuvre par:

– les instances médicales;
– les organismes de sécurité sociale et les administrations.

A leur propos, la licéité du traitement est garantie, *„lorsque le traitement de ces données est mis en oeuvre (…) par des personnes (responsable du traitement) soumises à une obligation de secret professionnel"* (considérant (33) de la Directive 95/46/CE et article 8 paragraphe (3) de la directive 95/46/CE).

C'est la relation de confiance „patient-médecin", assortie de la liberté dont dispose le patient de choisir son médecin, qui confère à ce dernier, ainsi qu'aux personnes qui l'entourent dans l'exercice de sa profession, le droit de traiter de façon licite les données relatives à la santé de ses patients. Ce droit bénéficie, par extension, à l'ensemble des activités liées à la santé publique.

Le corollaire de cette extension est l'extension de l'obligation au secret, car on ne peut permettre à l'ensemble des services de la santé publique ce que peut faire un médecin, sans que ce service ne soit soumis à une quelconque obligation de secret. Ainsi, le responsable du traitement des services de santé publique devra être soumis au secret professionnel, son sous-traitant respectera l'obligation de confidentialité.

c) *Les modalités de mise en oeuvre*

L'article 7 paragraphe (2) prévoit que les traitements seront soumis à la procédure de l'autorisation préalable de l'article 14.

Toutefois, l'article 7 paragraphe (3) prévoit, pour des raisons pratiques que la procédure sera celle de la notification ou de la désignation d'un chargé de la protection des données:

– lorsqu'un traitement est mis en oeuvre conformément l'article 36 de la loi du 28 août 1998 sur les établissements hospitaliers, ou

– lorsqu'il s'agit de la relation médecin-patient.

L'ordre des médecins aurait ainsi la possibilité de désigner un chargé de la protection des données.

De façon incidente, on rappellera que le patient a un accès à l'ensemble des données du dossier qu'il a auprès de son médecin (cf. supra III. 2. e) tiret 2 sur le droit d'accès).

C. *Les données judiciaires (article 8)*

Les traitements de données relatives aux infractions, aux condamnations pénales, ou aux mesures de sûreté, ne peuvent être effectués qu'en exécution d'une disposition légale (y compris la protection de la jeunesse).

Le recueil exhaustif des condamnations pénales (casier judiciaire) continue à être tenu sous le contrôle de l'autorité publique compétente de même que les données relatives aux jugements civils ou administratifs, ainsi qu'aux sanctions administratives.

D. *Les traitements de données à la liberté d'expression (article 9)*

a) *Définition*

La liberté d'expression est une notion large qui englobe l'expression artistique, littéraire en général et journalistique en particulier.

Il s'agit de concilier le droit à la vie privée avec les règles régissant la liberté d'expression.

b) *Limitation et exception des droits d'information et d'accès*

– Le journaliste doit disposer d'une certaine marge de manoeuvre et l'obligation d'informer la personne concernée ne lui est pas applicable, dans la mesure où elle compromettrait la collecte des données[1], la publication ou la mise à disposition du public ou encore permettrait l'identification des sources.

– Lorsque, de manière générale, il y a investigation de la Commission nationale pour la protection des données, celle-ci, dans le respect des règles relatives à la liberté d'expression, ne peut opérer qu'en présence de l'organe représentatif de la presse. Il appartient à la loi sur la presse en cours d'élaboration de préciser quel est cet organe représentatif. Ce dernier sera le garant du respect des obligations relevant du statut professionnel du journaliste.

1 Le journaliste pourrait voir sa collecte de données compromise s'il informait la personne concernée de son intention de rédiger un article destiné à démontrer, par exemple, que le taux d'analphabétisme est supérieur dans certains quartiers de la cité.

– Le droit d'accès et de rectification est également et exceptionnellement limité. La loi prévoit que dans ce cas la personne concernée ne dispose que d'un droit d'accès indirect, ceci par le biais de la Commission nationale pour la protection des données[1] (article 28 paragraphe (4)). Cette limitation au droit d'accès devra, le cas échéant, être motivée par le journaliste. En pratique, cette motivation prendra la forme d'une référence au droit à la liberté d'expression et au risque, qu'encourrait le journaliste dans l'exécution de sa tâche s'il donnait un accès à la personne concernée.

Afin que cette exception ne soit pas appliquée de façon arbitraire la personne concernée peut alors s'adresser à la Commission nationale pour la protection des données, pour que celle-ci procède, en son nom, aux vérifications nécessaires, tout en faisant opérer la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente loi.

Lors de communications avec la personne concernée, la Commission ne peut mettre en danger la ou les finalités des traitements (la liberté d'expression comme finalité ultime de tout travail de journalisme sera ainsi protégée). Ainsi, par exemple, elle ne pourra pas aller à l'encontre des droits du journalisme qui se réfugie derrière la jurisprudence de la Cour Européenne des Droits de l'Homme sur la protection des sources. Tout au plus pourra-t-elle communiquer le résultat de ses investigations sous forme d'appréciations générales à l'adresse de la personne concernée.

Notons que pour qu'un accès soit demandé, il faudra tout au moins, que la personne concernée soit informée de l'existence du traitement mis en oeuvre sous la responsabilité du journaliste. Ce journaliste dispose, comme nous l'avons vu (cf. supra premier tiret) et dans ce domaine également, d'instruments lui permettant de protéger sa fonction.

c) *La notification allégée*

Afin de ne pas mettre en danger, la liberté d'expression, la notification obligatoire auprès de la Commission d'un traitement effectué à des fins de journalisme ou d'expression artistique ou littéraire, ne renseigne que sur les nom(s) et adresse(s) du responsable du traitement ou de son représentant.

Là encore, aucune information ne sera délivrée au préjudice du droit à la protection des sources et, de façon générale, du droit à la liberté d'expression.

E. *Les traitements à des fins de surveillance (article 10)*

Le projet de loi inclut les traitements de données à des fins de surveillance comme par exemple la vidéosurveillance ainsi que toute autre forme de surveillance électronique. Il distingue entre le traitement de données à des fins de surveillance sur le lieu de travail (article 11) et d'autres hypothèses (article 10). Les obligations et autres règles prévues à charge du responsable du traitement et au bénéfice de la personne concernée ne sont jamais exclusives des autres dispositions protectrices du projet de loi. Il s'agit ici de l'application du droit commun.

a) *Les cas prévus*

Ces cas sont limitatifs. L'article 10 traite de toutes les formes de surveillance et en particulier de la vidéosurveillance et des nouvelles technologies. L'axe principal de cet article est la finalité du traitement.

Est autorisée la surveillance:

– si la personne concernée a donné son consentement exprès, ou
– par l'Etat dans son rôle de garant de la sécurité publique[2] lorsque cela est exclusivement et limitativement nécessaire à la prévention, la recherche, la constatation et à la poursuite d'infractions pénales, ou

1 Tant que les données auxquelles l'accès est demandé n'ont pas été publiées, leur communication ou toute information disponible sur leur origine ne peut se faire que par l'intermédiaire de la Commission.

2 Dans les parkings couverts, les gares et aérogares, les moyens de transports publics, aux abords ou dans tout autre lieu accessible ou non au public pourvu qu'il présente dans sa situation, sa configuration ou sa fréquentation un risque (…)

– dans les propriétés privées à des fins exclusivement domestiques. Il s'agit d'une facette de l'activité domestique des personnes physiques qui est hors du champ de la loi et ne saurait donc être réglementée (article 3 paragraphe (3) de la loi)[1].

L'hypothèse de la sécurité publique englobe bien entendu la circulation routière et les infractions de roulage. Les systèmes de surveillance par caméras sur la route sont donc possibles dans ce cadre. Par ailleurs, lorsqu'il s'agira de récolter des données relatives à la santé lors de l'exécution de missions générales remplies par les agents du Ministère des Transports, on se basera plutôt sur la dérogation à la prohibition de l'article 6 du projet de loi et fondée sur l'intérêt public important.

b) *La garantie supplémentaire: l'information spéciale*

Les paragraphes 2 et 4 rappellent et précisent l'obligation d'information notamment de l'article 26 tout en précisant certains aspects spécifiques à la surveillance. Cette information supplémentaire exigée par la loi prendra la forme d'une publicité qui s'adaptera à la nature même de la surveillance. Cette information pourra prendre la forme d'un affichage ou d'une circulaire, lorsque la surveillance porte sur un lieu qu'empruntent plusieurs personnes, ou encore la forme d'une notification individuelle, lorsque cela s'avère approprié (surveillance d'une seule personne quel qu'en soit le moyen). Référence est faite au recommandé par voie électronique, reconnu dorénavant au même titre que le recommandé par voie postale et qui pourra être utilisé comme mode d'information de la personne concernée.

Notons que lorsqu'il s'agira de la recherche, la constatation et la poursuite d'infractions pénales, les exceptions nécessaires à l'obligation d'informer la personne concernée joueront. La prévention ne bénéficie pas de cette exemption car lorsque l'on surveille exclusivement pour prévenir et non pour guérir, la publicité et l'information participent activement à cette fin.

c) *Une communication limitée des données issues de la surveillance*

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

– si la personne concernée a donné son consentement exprès, ou
– aux autorités publiques dans le cadre de la prévention, la recherche, la constatation et à la poursuite d'infractions pénales, ou
– aux autorités judiciaires compétentes pour constater et poursuivre une infraction pénale et celles devant lesquelles sera exercé ou défendu un droit en justice.

F. *La surveillance sur le lieu de travail (article 11)*

La surveillance sur le lieu de travail telle qu'envisagée ici est celle mise en oeuvre sous responsabilité de l'employeur. Rien n'exclut en effet, une surveillance dans le cadre de l'article précédent qui serait faite licitement par les services de police et qui se déroulerait dans une entreprise.

a) *Les cas d'ouverture*

Les cas d'ouverture permettant cette surveillance sont limitatifs. Le traitement à des fins de surveillance sur le lieu de travail ne peut être mis en oeuvre par l'employeur qui en est le responsable que s'il est nécessaire:

– pour les besoins de sécurité et de santé des travailleurs, ou
– pour les besoins de protection des biens de l'entreprise, ou
– pour le contrôle du processus de production portant uniquement sur les machines, ou
– pour le contrôle temporaire de production ou des prestations du travailleur en vue de mesurer son activité afin de déterminer sa rémunération.

Ainsi, on peut surveiller légalement par tout moyen, un employé lorsque l'on respecte certaines règles.

---

1 Rappelons que l'activité domestique d'une personne physique n'entre pas dans le champ d'application du projet de loi et qu'un traitement de données mis en oeuvre dans ce cadre est totalement libre.

Ces règles sont applicables à toute personne travaillant dans l'entreprise. L'utilisation du terme d'employé recouvre toutes les formes de contrats existants.

La première de ces règles est inscrite en filigrane. Le consentement de la personne concernée n'est pas prévu comme hypothèse de légitimation de la surveillance sur le lieu de travail. Ceci est nécessaire afin de protéger l'employé qui est dans une relation déséquilibrée avec son patron. Ce dernier s'il pouvait utiliser le consentement de son employé pourrait l'extirper trop aisément, pour l'insérer systématiquement dans le contrat de travail, et d'une protection on aboutirait à un affaiblissement de la protection.

La deuxième de ces règles également en filigrane est, vu le caractère limitatif des cas légitimant la surveillance sur le lieu de travail, que celle-ci ne pourra avoir pour finalité de limiter les possibilités d'un employé au maintien de son emploi ou à l'obtention de son emploi. Une telle utilisation serait en effet déloyale.

La troisième de ces règles est qu'un employé qui serait surveillé pour mesurer son activité afin de déterminer sa rémunération ne pourrait l'être que temporairement. Toute surveillance permanente d'un salarié à cette fin est donc exclue.

Les autres dispositions de l'article 11 portent sur l'information et la procédure.

b) *la garantie supplémentaire: l'information spéciale*

– les destinataires de l'information spéciale:

  Le projet de loi prévoit, sans préjudice du droit à l'information de la personne concernée, que le comité mixte, ou à défaut la délégation du personnel, ou à défaut encore l'Inspection du Travail et des Mines, seront spécialement informés par l'employeur de la mise en oeuvre de la surveillance. La transparence est un élément essentiel pour que le travailleur soit protégé. Cette protection passe par la vigilance des organes représentatifs de ses intérêts. Ceux-ci participeront au sein de l'entreprise à l'établissement d'un dialogue permettant de respecter les intérêts de chacune des parties.

– les informations spéciales porteront sur:
  * la finalité du traitement auquel les données sont destinées,
  * le cas échéant la ou les périodes pendant lesquelles la surveillance sera effectuée,
  * la durée et le cas échéant les conditions de conservation des données.

c) *Le régime de mise en oeuvre*

La dernière garantie et non la moindre est de prévoir que la surveillance sur le lieu de travail exigera une autorisation préalable de la Commission nationale pour la protection des données conformément à l'article 14 de la loi.

En outre, dans les société anonymes ayant des comités mixtes, ceux-ci seront compétents, conformément à l'article 7 paragraphes (1) et (2) de la loi du 6 mai 1974 instituant des comités mixtes dans les entreprises du secteur privé et organisant la représentation des salariés dans les sociétés anonymes. Ce sont donc eux qui autoriseront la surveillance, lorsqu'elle est mise en oeuvre pour la sécurité et la santé des travailleurs et pour le contrôle temporaire de production ou des prestations du travailleur.

La rédaction de codes de conduites éclairant l'employeur et lui servant de vade-mecum serait la bienvenue.

G. *Le cas spécial du répertoire téléphonique (article 41)*

L'article 41 est une exception aux principes énoncés dans la présente loi dans la mesure où il oblige les opérateurs de télécommunications et/ou postaux ainsi que leurs fournisseurs de services de permettre l'accès à certaines données relatives à leurs abonnés et aux services de ceux-ci.

Les autorités légales (procureur, parquet services de secours …) s'adressent par voie électronique au centre d'information (ILR) qui vérifie si le requérant est autorisé à formuler la requête. Cette requête est transmise par l'intermédiaire de systèmes informatiques appelés „black box“ (boîtes noires installés auprès des opérateurs et/ou fournisseurs de services). Par ce mécanisme, l'opérateur et/ou le fournisseur de services n'est pas en mesure de savoir si une requête a été transmise ni à propos de quel client elle a été introduite.

Aucune base de données centralisées n'est créée et donc la discrétion et la confidentialité sont garanties, la procédure permet l'exécution en temps réel, ce qui permet par exemple de gagner du temps précieux dans le cas d'une prise d'otage.

Les personnes, agissant dans le domaine de la sauvegarde de la vie et autorisées de plein droit, seront définies dans le cadre d'un code de conduite, approuvé par la Commission nationale pour la protection des données.

L'automatisation complète de la procédure exige l'autorisation de la Commission nationale pour la protection des données. La Commission vérifiera particulièrement la sécurisation du système, qui devra être conforme aux exigences des articles 22 et 23 de la loi.

III. 4. Les procédures

Une fois l'ensemble des cas de traitement ainsi que les droits des personnes concernées analysée, il convient de décrire les procédures applicables à la mise en oeuvre des traitements.

Le double impératif qu'est la libre circulation conjuguée à la protection de la personne concernée s'applique aussi bien aux personnes privées qu'aux personnes publiques à savoir les administrations qui auront à traiter des données à caractère personnel. Dès lors les règles et les procédures seront les mêmes pour les acteurs du secteur public comme pour ceux du secteur privé et en principe, un traitement de données à caractère personnel pourra être librement mis en oeuvre. Une simple formalité de notification[1] sera effectuée auprès de la Commission nationale pour la protection des données. La notification s'apparente à une obligation de déclaration à l'organisme chargé de vérifier, a posteriori, le respect de la loi. Toutefois, dans certains cas le responsable du traitement sera exempté de cette obligation de notification.

a) *Les exemptions à l'obligation de notification (art. 12 paragraphe (2))*

– Le responsable du traitement peut au lieu de correspondre avec la Commission nationale pour la protection des données et donc au lieu de lui notifier directement ses traitements, désigner un *chargé de la protection des données* (cf. infra) tenu d'assurer l'application des dispositions légales en la matière et d'établir un registre des traitements conformément à l'article 15. Le chargé de la protection des données est un auxiliaire de la loi. Son contrôle se fera de façon indépendante. La désignation d'un interlocuteur privilégié par un responsable du traitement permettra une meilleure prise en compte de ses besoins mais également une application moins rigide de la loi et par conséquent une meilleure assimilation. Cette exemption est essentielle et se base sur une forme encadrée d'autorégulation ou tout au moins de collaboration active au respect des dispositions légales.

– Les traitements ayant pour seul objet 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 n'ont pas besoin (vu leur caractère) d'être notifiés. Ainsi par exemple le registre du commerce n'est pas soumis à cette sujétion et ne devra ni être notifié ni connaître de publicité.

– Les traitements de données soumis à l'autorisation par voie réglementaire (cf. infra article 17). Le règlement est une mesure de publicité suffisamment forte pour pouvoir se substituer aux autres règles.

– Les traitements de données mis en oeuvre conformément aux règles de procédures judiciaires ne doivent pas être notifiés. Cela s'impose afin de ne pas perturber le bon déroulement de la justice et alors que le principe du contradictoire, celui du procès équitable remplissent la plupart des fonctions attribuées à la protection des données.

1 Il y a toutefois maintien de l'autorisation préalable pour un certain nombre de traitements, notamment de données sensibles, ceux mis en oeuvre par les forces de l'ordre et les services de sûreté de l'Etat, les traitements pour lesquels, pour des raisons évidentes, il existe par ailleurs des limitations, voire des exceptions aux droits des personnes concernées (cf. infra dans le texte).

b) *La notification (art.12, 13)*

– *Le contenu de la notification:*

Cette notification comportera des informations précises et relatives au fonctionnement du traitement:

* le nom et l'adresse du responsable du traitement ou de son représentant et le cas échéant du sous-traitant;
* la ou les finalités du traitement;
* la description de la ou des catégories de personnes concernées et des données ou des catégories de données s'y rapportant;
* les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
* les pays tiers à destination desquels des transferts de données sont envisagés;
* 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;
* la durée de conservation des données.

Notons qu'aucune de ces informations ne concerne l'identité des personnes concernées. Le but de cette notification est de permettre à la Commission nationale pour la protection des données de vérifier, a posteriori, la conformité du traitement à la loi. Il ne s'agit pas de créer, un super-fichier des personnes fichées, dont la mise en place exigerait des efforts disproportionnés et dont l'efficacité serait assurément mauvaise. En effet, outre le risque de dérive, inhérent à la mise en place d'un tel super-fichier, on se noierait indubitablement sous le nombre d'informations.

– *publicité suite à la notification du traitement (art. 15)*

La Commission nationale pour la protection des données tiendra un registre des traitements à elle notifiées.

A l'unité de la règle de la notification répondent deux exceptions essentielles constitutives de régimes d'exception basés sur un système d'autorisation préalable.

c) *L'autorisation préalable (article 14)*

La procédure de l'autorisation préalable subsiste chaque fois que le traitement de données à caractère personnel présente un risque intrinsèque, d'atteinte au respect de la vie privée de la personne concernée, au regard de la nature des données traitées et de la finalité du traitement[1]. L'autorisation sera sollicitée auprès de la Commission nationale pour la protection des données.

La Directive 95/46/CE dans son article 20 paragraphe 3, autorise les Etats à substituer au contrôle de la Commission, l'autorisation de la loi. Il ne s'agit pas d'une permission de déroger aux règles de droit contenues dans la Directive, respectivement dans le projet de loi. Il ne s'agit que d'une procédure alternative d'autorisation d'un traitement de données à caractère personnel. Une loi qui autoriserait un traitement de données soumis en principe à l'autorisation préalable de la Commission, resterait soumise au règles de la Directive 95/46/CE. Une telle loi ne saurait dès lors, limiter les droits positifs attribués par cette directive aux sujets de droit. Il ne faut donc pas y voir une solution pratique. Au contraire, chacune de ces lois devra prévoir des garanties similaires à celles du présent projet de loi, et une expertise longue et fastidieuse sera nécessaire. De plus conformément à l'article 34 paragraphe (3) (e) l'avis de la Commission nationale pour le protection des données sera nécessaire. En optant pour le système de l'avis la relation se limitera au seul avis rendu. Au contraire, s'en remettre à l'autorisation de la Commission permet une relation constructive avec un organisme spécialisé et avec lequel une négociation sera toujours possible pour trouver une solution qui satisfasse les intérêts en présence et les exigences de la loi.

1 Un traitement de données concernant la solvabilité ou le crédit d'un client d'un professionnel du secteur financier sera soumis à autorisation préalable car il conditionne les relations économiques, l'octroi d'un droit ou la signature d'un contrat au bénéfice de la personne concernée. Ceci ne remet pas en cause la nécessité de tels traitements mais vise à protéger la personne concernée.

L'autorisation une fois donnée fera l'objet de la même publicité au registre des traitements que celle prévue pour un traitement soumis à notification.

Le traitement constitué par une interconnexion (article 16) sera soumis à l'exigence d'une telle autorisation préalable alors qu'une interconnexion exige que l'on vérifie précisément la compatibilité entre les finalités des traitements interconnectés. Ce principe de finalité est, rappelons, le principe fondateur du projet de loi. Il ne serait pas opportun d'ouvrir, par le biais de l'interconnexion, une brèche dans ce principe fondamental.

La question de l'interconnexion dans son acception traditionnelle est encore aujourd'hui d'actualité car toutes les grandes structures économiques et sociales désirent encore „croiser leurs fichiers". Toutefois, il n'est plus techniquement nécessaire d'interconnecter à proprement parler de grandes bases de données, pour compléter et créer un super fichier universel. Le phénomène, déjà existant, de la décentralisation des informations et de leur disponibilité à être regroupées en un instant par des moteurs de recherche, permet d'obtenir le même résultat, soit une information universelle sur telle ou telle personne. Les deux mécanismes coexistent aujourd'hui.

Il était donc opportun de donner une définition large de l'interconnexion comme une opération visant, quelqu'en soit le mode, à corréler entre elles des données traitées dans des finalités différentes.

d) *L'autorisation préalable par voie de règlement grand-ducal (art. 17)*

Des procédures spéciales régiront les activités de l'Etat qui sont strictement régaliennes (police, sûreté, matière pénale). En effet, la puissance publique a des impératifs qui exigent l'aménagement de certaines procédures et de certaines règles. De tels traitements resteront sous le contrôle de l'exécutif qui les autorisera par voie de règlement grand-ducal.

Ainsi, conformément à l'esprit de la Directive 95/46/CE, le projet de loi concilie la mise en place d'un régime juridique unique soumettant tous les aspects de l'activité humaine tout en sauvegardant d'une part l'intérêt de l'Etat et d'autre part, en préservant prioritairement la vie privée de chacun, adoptant ça et là les procédures spéciales nécessaires.

Sous forme de tableau récapitulatif, les procédures sont ventilées de la façon suivante:

Procédures applicables à la mise en oeuvre des traitements de données à caractère personnel

Procédure applicable à la mise en oeuvre du traitement de données à caractère personnel *Types de traitements de données à caractère personnel*	*Notification à la CNPD (article 12)*	*Autorisation préalable de la CNPD (article 14)*	*Autorisation par voie de RGD (article 17)*	*Autorisation d'une loi*
Droit commun pour tout type de traitements (articles 4 et 5)	Principe	Exceptions: 1. traitements ultérieurs de données à des fins statistiques, historiques ou scientifiques (article 4 (2)) 2. traitement concernant le crédit et la solvabilité de la personne concernée (article 14 (1) (d)) 3. utilisation de données à des fins autres que celles pour lesquelles elles ont été collectées (article 14 (1) (e))		
Traitement de catégories particulières de données (articles 6 et 7)	Exceptions: 1. Sauvegarde de la vie de la personne concernée ou d'un tiers (article 6 (2) (c)), 2. article 36 de la loi du 28 août 1998 sur les établissements hospitaliers (article 7 (3)) 3. relation médecin-patient (article 7 (3)) 4. journalisme, expression littéraire, artistique (article 9 (1) (a))	Principe		Exception: Traitement mis en oeuvre lors de la constatation, de l'exercice ou de la défense d'un droit en justice (article 6 (2) (f)): voir *procédures judiciaires et principe du contradictoire*
Traitement de données judiciaires (article 8)				Casier et organisation judiciaire

Procédure applicable à la mise en oeuvre du traitement de données à caractère personnel *Types de traitements de données à caractère personnel*	*Notification à la CNPD (article 12)*	*Autorisation préalable de la CNPD (article 14)*	*Autorisation par voie de RGD (article 17)*	*Autorisation d'une loi*
Traitement à des fins de surveillance (article 10) ainsi que surveillance sur le lieu de travail (article 11)	Principe de l'article 10	Principe de l'article 11	Exception à l'article 10: Dans les parkings couverts, les gares (…) s'ils sont nécessaires à la prévention, la recherche et la poursuite d'infractions pénales (article 10 (1) (b) dans la champ de l'article 17)	
Traitement nécessaire à la prévention, la constatation, la poursuite d'infractions pénales, la sûreté de l'Etat, la défense, la sécurité publique (article 17 (1) et (2)			Principe (article 17)	
Traitement constitué par l'interconnexion de données à caractère personnel (article 16)		Principe	un règlement grand-ducal pourra déterminer les modalités de mise en oeuvre du traitement (article 16 (3))	

III. 5. La Commission Nationale pour la Protection des Données

Le projet de loi a choisi de soumettre les différentes catégories de traitement de données à des procédures de contrôle les moins contraignantes possibles tout en assurant un niveau de protection adéquat aux personnes concernées. Il s'agissait également, de ne pas entraver la libre circulation des données à caractère personnel et par là, le développement de certains domaines tels que le commerce électronique.

Ainsi, les garanties des droits fondamentaux et du respect de la vie privée se nomment droit d'information, droit d'accès, droit de rectification et droit d'opposition. Ces garanties ont été prévues au bénéfice de la personne concernée par un traitement de données à caractère personnel.

Les garants du respect des droits fondamentaux et en particulier de la vie privée sont la Commission nationale pour la protection des données et/ou le chargé de la protection des données.

La loi du 31 mars 1979 prévoyait un contrôle a priori systématique de la commission consultative, suivi de l'autorisation du ministre. L'article 28 de la Directive 95/46/CE prévoit l'instauration d'une autorité de contrôle dotée d'un pouvoir de contrôle plus étendu que celui prévu par la loi du 31 mars 1979.

a) *Le statut et l'indépendance*

La Commission est une autorité indépendante qui prend la forme d'un établissement public doté de la personnalité juridique et d'une autonomie administrative et financière.

Pour effectuer le contrôle de la loi, la Commission est dotée des pouvoirs d'investigation et d'intervention nécessaires à l'exercice en toute indépendance de ses missions. La Commission sera à l'avenir le garant pour une application correcte de la présente loi.

Le statut garantit l'indépendance de la Commission. Cette indépendance repose sur l'octroi de la personnalité juridique et sur certaines incompatibilités. Ainsi, la fonction de membre de la Commission ne pourra se cumuler avec certaines autres fonctions comme celles de membre du Gouvernement, de la Chambre des Députés, du Conseil d'Etat ou du Parlement européen. Dans le même ordre d'idées, un membre de la Commission ne pourra exercer d'activités professionnelles ou détenir directement ou indirectement des intérêts dans une entreprise ou tout autre organisme opérant dans le champ des traitements de données à caractère personnel. De plus, dans l'exercice de leurs fonctions, les membres et les suppléants de la Commission ne reçoivent d'instruction d'aucune autorité.

b) *Le chargé de la protection des données (article 40)*

La configuration de la Commission nationale pour la protection des données (3 membres, effectif réduit) ne permettra pas que la protection des données soit gérée de façon centralisée. Tel n'est pas l'objectif de la Directive, tel ne devra pas être la voie suivie par le législateur luxembourgeois. Un choix hypercentralisé serait en effet voué à l'échec et la paralysie. La gestion de la protection des personnes concernée par un traitement ne peut-être que décentralisée.

A cette fin, le projet de loi prévoit que le responsable du traitement peut nommer un chargé de la protection des données. Cette institution se substitue à la Commission nationale pour la protection des données. Le chargé de la protection désigné devient le destinataire des notifications des traitements mis en oeuvre par son responsable du traitement[1].

La Commission nationale pour la protection des données jouera le rôle de „conseil des sages": La Commission adaptera la pratique à chaque situation, la rendra cohérente au regard de la loi et donnera suite aux plaintes des personnes lésées dans leurs droits. Les chargés de la protection des données feront l'interface entre la Commission nationale pour la protection des données et les responsables de traitements. Ces interfaces permettront la bonne application de la loi.

1 L'article 18 paragraphe (2) de la Directive prévoit que l'on peut substituer à l'autorité de contrôle un détaché à la protection des données. Ce détaché se nomme „chargé de la protection des données" dans la loi.

Ainsi, le chargé de la protection des données doit, à l'instar de la Commission, *„assurer de manière indépendante l'application interne des dispositions nationales prises en application de (…) la Directive (et) tenir un registre des traitements effectués par le responsable du traitement (…)"*[1]. Ces missions qui se substituent en grande partie à celles de la Commission ne peuvent être effectuées que de façon indépendante[2]. La garantie de cette indépendance nécessite d'interdire tout lien de subordination entre le responsable du traitement et le chargé de la protection des données. Ainsi, ces deux acteurs ne pourront pas être liés par un contrat de travail alors qu'un des critères définissant ce type de contrat est l'existence même d'un lien de subordination.

c) *La composition de la commission (article 36)*

C'est un organe collégial composé de trois membres à temps plein et de trois suppléants dont un président et un vice-président nommés sur proposition du Gouvernement en conseil. Parmi les membres effectifs, il y aura au moins un informaticien et un juriste.

d) *Les missions de la Commission (article 34)*

La mission principale de la Commission consiste à contrôler et à vérifier si les données à caractère personnel soumises à un traitement sont traitées en conformité avec les dispositions de la présente loi et de ses règlements d'exécution. Ce contrôle est fait a posteriori.

Ce contrôle auquel est soumis l'Etat, les personnes publiques, les secteurs clefs de l'économie exige, conformément à la Directive 95/46/CE, une indépendance structurelle et fonctionnelle très poussée qui permet à la fois d'éviter les abus directs et de protéger le secteur privé de toute tentative d'ingérence de l'Etat. Cette indépendance a pour corollaire la soumission au secret professionnel des membres et agents de la Commission[3].

L'indépendance de la Commission lui donne une place privilégiée pour intervenir dans d'autres formes de régulations telles que la corégulation ou l'autorégulation. Ainsi, elle pourra recevoir et le cas échéant après discussion avec les auteurs approuver les codes de conduite relatifs à un traitement ou un ensemble de traitements qui lui sont soumis par des associations professionnelles représentatives de responsables du traitement.

e) *Les pouvoirs (articles 34 et 35)*

La Commission peut délivrer des sanctions administratives sous forme d'amendes d'ordre, d'admonestations ou d'avertissements au responsable du traitement.

Elle pourra également:

– verrouiller, effacer ou détruire des données faisant l'objet d'un traitement contraire aux dispositions de la présente loi et/ou de ses règlements d'exécution;
– interdire temporairement ou définitivement un traitement contraire aux dispositions de la présente loi et/ou à ses règlements d'exécution;
– ordonner l'insertion intégrale ou par extraits de la décision d'interdiction dans un ou plusieurs journaux quotidiens aux frais de la personne condamnée.

A ces fins, la Commission 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. Elle a un accès direct aux locaux où a lieu le traitement et procède aux vérifications nécessaires.

---

1 Article 18 paragraphe (2) tirets 3 et 4 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données.

2 Article 40 paragraphe 4 du projet de loi et 18 paragraphe (2) tiret 3 de la directive 95/46/CE.

3 A ce propos on relèvera que la Commission limitée par la finalité de son action qu'est la protection des données et liée par le secret professionnel agira dans le respect des intérêts de la place financière.

III. 6. Les recours

a) *La Commission*

Toute personne peut saisir la Commission si elle se croit lésée dans un de ses droits et libertés fondamentaux dont celui à la vie privée, par la mise en oeuvre d'un traitement de données la concernant.

b) *Les recours de droit commun (article 32)*

On ne fait que renvoyer à l'éventail des procédures existantes dans le droit commun s'agissant des actions devant l'ordre judiciaire.

Un dommage appelle une réparation, qu'elle soit privée ou publique, et donc que l'instance soit civile ou pénale. Dans le même ordre d'idées, une voie de fait appelle une mesure de conservation provisoire ou définitive.

c) *Le recours rapide spécifique (article 33)*

Le dispositif de droit commun est complété par une procédure rapide. Cette procédure vise à suspendre les droits d'un responsable du traitement ayant manifestement violé les dispositions de la loi relatives à la procédure de mise en oeuvre et à la publicité.

On appréhende ici le responsable du traitement dans son attitude positive en rapport avec ses obligations les plus élémentaires.

Il s'agit de donner un signal clair et non équivoque avertissant et sanctionnant immédiatement certains comportements pour que les responsables de traitements prennent conscience de leurs obligations et du cadre légal mis en place.

d) *Les sanctions pénales*

Chaque principe édicté dans le projet de loi est accompagné d'une sanction pénale. En effet, les règles sont d'ordre public et l'on touche aux droits et libertés fondamentaux des personnes concernées par les traitements de données. En outre, au sortir d'un régime peu actif, il faut rappeler aux acteurs de la loi leurs responsabilités. Enfin, le projet de loi laisse une marge d'appréciation large au juge, la fourchette des amendes étant très large afin de lui permettre de s'adapter à la multitude des situations à venir et aux besoins de la répression.

III. 7. Le transfert vers des pays tiers (articles 18 à 20)

Le transfert de données vers des pays tiers à l'Union Européenne n'est possible que si ces pays respectent un niveau équivalent de protection des personnes concernées. Ceci s'analyse au cas par cas tant au niveau national qu'au niveau communautaire. On pourra tout de même transmettre des données vers un pays ne garantissant pas un tel niveau de protection: ex. en matière d'exécution d'un contrat auquel la personne concernée est elle-même partie ou si le destinataire installé dans le pays tiers s'engage à une telle protection ou encore s'il en va de la sauvegarde de la liberté d'expression.

On ne doit museler un journaliste parce que le pays vers lequel il voudrait communiquer des données personnelles ne respecte pas les droits de l'homme. En effet, c'est dans ces pays qu'il est particulièrement important que le journaliste puisse exercer librement son métier.

*

CONCLUSION

L'objectif du projet de loi est de fixer un cadre commun aux entreprises, aux particuliers et à l'Etat afin de permettre la circulation des informations, à travers les nouveaux réseaux, tout en adoptant une protection en adéquation avec les nouvelles technologies.

L'évolution rapide des moyens de communication, exige des règles rattachées à des concepts évolutifs. Ces concepts permettent l'attribution de droits positifs clairs, dans le chef des personnes concernées par les traitements (droit d'accès, d'opposition …), et d'obligations dans le chef des responsables de traitements (devoir d'information, de notification …). Ces obligations, une fois mises en pratique, offriront à la Commission nationale pour la protection des données suffisamment de transparence pour qu'elle coordonne et améliore au fur et à mesure le fonctionnement du système.

Pour réaliser ce but la Commission nationale pour la protection des données devra pouvoir s'appuyer sur les auxiliaires que sont les chargés de la protection des données, ainsi que sur l'outil sectoriel que sont les codes de conduites.

Ces codes de conduites, devront permettre l'émergence, entre réglementation et pratique, d'une forme de corégulation, nécessaire à l'environnement actuel.

Ils seront le lien entre la règle impersonnelle incluse dans la loi et la diversité de la société moderne. Ils permettront l'adaptation régulière des pratiques en la matière.

4735/01

N° 4735[1]

CHAMBRE DES DEPUTES

Session ordinaire 2000-2001

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

AVIS DE LA CHAMBRE DES FONCTIONNAIRES ET EMPLOYES PUBLICS

(22.5.2001)

Par dépêche du 15 décembre 2000, Monsieur le Ministre délégué aux Communications a demandé l'avis de la Chambre des Fonctionnaires et Employés publics sur le projet de loi spécifié à l'intitulé.

Le projet a pour but de transposer en droit luxembourgeois la directive 95/46/CE du Parlement Européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

A l'heure actuelle, la protection des données (malgré l'encadré figurant à la page 4 de l'exposé des motifs, la Chambre est d'avis que cette notion ne constitue pas un *„usage linguistique incorrect"* puisqu'il s'agit aussi de protéger les données nominatives devant tout abus qui risque d'en être fait) se trouve réglée, sur le plan national, par la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, modifiée à plusieurs reprises depuis lors. En raison de l'évolution du cadre juridique international ainsi que du véritable bouleversement qui s'est produit ces deux dernières décennies sur le plan des techniques de l'information et de la communication, les auteurs du projet sous avis ont toutefois choisi d'abandonner, c'est-à-dire d'abroger la loi précitée et d'élaborer un tout nouveau projet qui non seulement tient compte des prescriptions impératives de la directive 95/46/CE, mais qui, par endroits, va beaucoup plus loin et touche des domaines aussi divers que la santé, la justice (prévention de délits et criminalité), la presse, le droit du travail, la sûreté de l'Etat et la défense, etc.

*

REMARQUES LIMINAIRES

Ce qui frappe à la première lecture du projet, c'est précisément ce caractère de pêle-mêle et de fourre-tout. Associé au fait qu'il s'agit d'une matière d'une très haute technicité, dont la réglementation présuppose nécessairement l'emploi d'un style et d'un vocabulaire adaptés, cela débouche inévitablement sur un texte lourd et indigeste, pratiquement inintelligible pour le commun des mortels.

S'y ajoute que les auteurs raffolent visiblement de la technique du renvoi à d'autres dispositions de la même ou d'autres lois, de sorte que le projet ne comporte pratiquement aucun article qui ne fasse référence à un autre article. A titre d'exemple, l'article 27(2) prévoit que *„les dispositions de l'article 26(!) sont susceptibles de dérogations … dans les conditions prévues à l'article 9 paragraphe (1)(c)"*. La Chambre est parfaitement consciente qu'il est quasi impossible d'élaborer un projet de loi sans avoir recours à ce genre de technique, mais le texte sous avis semble l'utiliser partout où il y avait possibilité de le faire, de sorte que la Chambre a compté une petite centaine de renvois sur un total de 45 articles. Un autre exemple frappant se trouve à l'article 6(4)(a), qui renvoie à 6 dispositions différentes, dont aussi l'article 6(2)(h), cette dernière disposition renvoyant à son tour à l'article 17 qui, lui, fait référence à l'article 22! Un lecteur non averti pourrait avoir l'impression d'être exposé à un véritable *„harcèlement législatif"* voire à un *„mobbing textuel"*.

Enfin, toujours dans ce contexte, la Chambre se pose des questions sur la raison d'être d'une autre habitude ou *„technique législative"* couramment utilisée à tort et à travers dans tout le projet, et qui consiste à énoncer, en quelques lignes, un principe pour consacrer ensuite des alinéas et des alinéas, voire des pages entières, à l'énumération des exceptions et dérogations à ce principe. Tel est notamment le cas pour les articles 6, 12 et 18/19.

*

OBSERVATIONS PONCTUELLES

Ceci dit, la Chambre des Fonctionnaires et Employés publics voudrait commenter plus en détail certains aspects ponctuels du projet avant de procéder à un bref examen des articles. Cette approche lui paraît indiquée dans la mesure où certains points restent à clarifier voire méritent d'être différemment abordés.

*

LE BUT DU PROJET

Le but premier de la directive 95/46/CE, donc implicitement aussi celui du projet sous avis, consiste à garantir la libre circulation de l'information entre les Etats membres de l'Union Européenne dans le cadre du marché commun et à garantir dans ce contexte les droits et libertés de la personne humaine.

Avec l'emprise grandissante et irrésistible de l'ordinateur sur tous les domaines de la vie – publique et privée – la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel revêt aujourd'hui une signification et une importance autrement plus importantes qu'au moment où la loi du 31 mars 1979 a été élaborée, époque où seuls quelques gros ordinateurs, avec des données localisées, étaient en service, surtout au niveau de l'administration étatique, où l'interconnexion entre ces divers systèmes était pratiquement inexistante et où l'ordinateur personnel, le *„PC"* omniprésent aujourd'hui, restait à inventer.

La Chambre se demande dès lors si la protection des données ne mérite pas aujourd'hui d'être inscrite dans la Constitution, au même titre que l'inviolabilité du domicile et le secret des lettres. Ce qui est en tout cas inquiétant en l'occurrence, c'est que les *„droits de la personne concernée"* en tout premier lieu ne figurent qu'au chapitre VI du projet (articles 26 à 31 sur un total de 45), comme s'il ne s'agissait que d'un aspect secondaire!

L'informatique est aujourd'hui omniprésente dans la vie au point que la très grande majorité de la population – tout en le sachant très bien! – ne s'en rend plus consciemment compte. Le simple fait de régler ses dépenses de consommation courantes par des moyens de paiements électroniques (cartes de crédit, minicash, online-banking), l'emploi d'un système GPS dans une voiture automobile ou l'utilisation d'un GSM permettent de déterminer avec exactitude qui se trouvait où et quand (*„tracing"*)!

Le numéro national d'identité est utilisé par les administrations communales (registres de l'état civil et bureau de la population), les contributions, la sécurité sociale (caisses de maladie et de pension, prestations familiales, assurances accident et dépendance), le Ministère des Transports (permis de conduire) et même des entreprises privées (Société nationale de contrôle technique des automobiles).

Du fait que la loi de 1979 a manqué de tenir le pas avec l'évolution fulgurante de la technologie informatique, très peu de gens savent aujourd'hui que la plupart des banques de données fonctionnent dans la plus parfaite illégalité. Ainsi, selon les informations dont dispose la Chambre, même les registres de la population gérés par les administrations communales par exemple le seraient sans base légale formelle, à moins que les dispositions y relatives de la loi électorale ne soient considérées comme suffisantes.

Même si base légale il y avait, des incertitudes subsistent: le mariage civil par exemple étant célébré publiquement, ce fait autorise-t-il voire oblige-t-il le fonctionnaire communal à informer M. X, sur simple requête téléphonique de celui-ci, si Mme Y est mariée et à qui?

*

LE CHAMP D'APPLICATION DE LA NOUVELLE LOI

Comme la Chambre l'a déjà écrit au début du présent avis, le projet touche une multitude de domaines (sécurité publique, défense, droit pénal, sûreté de l'Etat, santé, liberté d'expression, droit du travail) relevant de champs d'application différents (secteur privé/secteur public, national/européen/tiers-monde, personnes physiques/personnes morales), à objectifs parfois totalement dissemblables (relevés statistiques, surveillance sur le lieu de travail, prévention de la criminalité, fins publicitaires).

La question qui se pose dès lors est celle de savoir si certaines de ces dispositions n'auraient pas plutôt leur place dans la législation spécifique réglementant leur domaine, c'est-à-dire par exemple celles relatives à la liberté d'expression seraient à insérer dans la nouvelle loi sur la presse, actuellement en voie d'élaboration, celles sur la surveillance au lieu de travail seraient à incorporer dans la législation relative au droit du travail etc.

Une telle façon de procéder aurait en tout cas l'avantage d'alléger tant soit peu le projet sous avis, surchargé dans sa version actuelle, surtout en comparaison de la loi du 31 mars 1979 qu'il doit remplacer.

*

L'APPLICATION A LA FONCTION PUBLIQUE

Le texte proprement dit du projet ne précise nulle part expressis verbis que le champ d'application de la future loi englobe aussi la fonction publique. Tel ne fait cependant aucun doute au regard de l'affirmation de l'exposé des motifs selon laquelle *„le secteur public est soumis à la loi"*.

Or, les auteurs du projet semblent avoir oublié qu'il y a des différences fondamentales entre les secteurs public et privé qui font que toute disposition concernant l'un n'est pas forcément transposable à l'autre et vice versa.

Ainsi, le *„traitement à des fins de surveillance sur le lieu de travail"*, prévu à l'article 11, et sur lequel la Chambre reviendra ci-après, devrait se heurter au statut général des fonctionnaires de l'Etat, qui ne permet pas de mesurer la *„productivité"* du fonctionnaire afin de déterminer sa rémunération. De même, des mots comme *„comité mixte d'entreprise"* ou *„délégation du personnel"* sont des notions étrangères au secteur étatique proprement dit, où l'*„Inspection du Travail et des Mines"* n'est par ailleurs pas compétente.

En plus, le fait qu'il n'y aura plus de distinction entre secteur public et économie privée soulève un certain nombre d'insécurités et de questions pour le premier nommé.

Ainsi, sous le régime actuel, les banques de données étatiques doivent être autorisées par la voie légale ou réglementaire. Sous l'empire de la nouvelle loi, une simple notification suffira. Bien que ce procédé allège la procédure, certaines incertitudes restent.

Ainsi appartiendra-t-il par exemple au responsable du traitement (ministère ou administration?) de définir la finalité de son traitement et ce dernier sera seul responsable de la bonne exécution. Ne faudrait-il pas prévoir, par voie de règlement grand-ducal par exemple, une procédure spécifique comme la publication des traitements, une procédure de notification?

Le fonctionnaire pourra-t-il, voire devra-t-il refuser d'effectuer les traitements dont il croit qu'ils sont contraires à la finalité (définie par le responsable) ou bien devra-t-il exécuter les ordres de son supérieur hiérarchique?

Quel sera le statut du chargé de la protection des données pour le secteur public prévu aux articles 14 et suivants? La Chambre est d'avis qu'une distinction avec le secteur privé s'impose. La directive ne l'interdit pas, alors qu'il est loisible à l'Etat de fixer pour lui-même des règles plus strictes.

*

LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES

Les dispositions relatives à la Commission sous rubrique sont une énigme.

Sa composition

Si l'on connaît la prédilection du Gouvernement pour instituer tous azimuts des commissions, des groupes de travail, des cercles de penseurs, etc., dont le rendement est dans la majorité des cas inversement proportionnel au nombre – toujours imposant – d'*„experts"* qui les peuplent, l'on pourrait à première vue se réjouir d'un organe limité à trois membres effectifs et trois membres suppléants. Toutefois, au regard de l'importance capitale et, surtout, du nombre et du volume des tâches que lui confie l'article 34, l'on reste stupéfait devant l'optimisme à la base de ce choix.

A moins que l'intention cachée n'ait été de rendre inopérante la Commission dès son institution – ce dont la Chambre doute – les effectifs prévus sont tout simplement insuffisants, pour ne pas dire ridicules.

Si la Commission travaillait en permanence à six membres (3 effectifs et 3 suppléants), il y aurait peut-être une chance qu'elle s'en sorte. Tel n'est cependant pas le cas puisque le commentaire de l'article 36 parle d'un nombre *„impair"*. L'on est donc en présence d'une Commission Nationale pour la Protection des Données de trois membres *„dont un président et un vice-président"!* La Chambre demande que cette composition soit revue et corrigée dans le sens que la Commission puisse fonctionner efficacement.

Son statut

Quant au statut de la Commission, la Chambre est consciente de la nécessité de lui conférer une totale indépendance et une autonomie administrative et financière. La Chambre voudrait cependant dans ce contexte rappeler ses réserves traditionnelles et bien connues quant au caractère *d'„établissement public"* qu'il est prévu de lui conférer.

Son personnel

Il est de même incompréhensible et inacceptable que *„les membres (!) et agents de la Commission"* soient *„des employés privés à assimiler à des employés de l'Etat"*.

Pour être *„employé privé"*, il faut d'abord un employeur. Or, l'employeur est la Commission. Les membres de la Commission – nommés par le Grand-Duc! – seraient donc leurs propres employés privés?

Quant aux *„agents nommés et placés sous son autorité"*, la Chambre se demande si la prestation du serment prévu au paragraphe (3) de l'article 38 peut être exigé d'un employé privé.

Enfin, si lesdits agents sont déjà employés privés, le paragraphe (5) du même article est un parfait non-sens puisqu'il dispose que *„le cadre du personnel de la Commission pourra être complété par … des employés"!* Et comme si cela n'était pas suffisant, le paragraphe (6) prévoit le recours *„à des experts externes engagés sur base d'un contrat de droit privé"*. Comprenne qui pourra!

Son fonctionnement

Selon le paragraphe (1), la Commission sera libre d'élaborer son règlement intérieur sans l'intervention de qui que ce soit, donc à son entière discrétion. La Chambre des Fonctionnaires et Employés publics ne voudrait que rappeler dans ce contexte que même le règlement d'ordre interne des chambres professionnelles est soumis, aux termes de l'article 23 alinéa 2 de leur loi organique, *„à l'approbation du Gouvernement"!*

L'article 37 (2) (c) du projet prévoit que le règlement intérieur de la Commission fixera *„les modalités de désignation du président et du vice-président"*. Or, selon l'article 36 (2), ceux-ci seront *„nommés par le Grand-Duc pour un terme de six ans renouvelable une fois"*. Quelles autres *„modalités"* restent alors à fixer?

Selon le paragraphe (4) de l'article 37, la majorité des membres *„en exercice présents ou suppléés"* doivent participer à la séance pour que la Commission puisse valablement délibérer. Cela en fait donc deux sur trois. La Chambre ne voit dans ce cas pas l'utilité de différencier selon *„la majorité"* des voix, la *„majorité absolue"* et la *„majorité d'au moins deux voix"*, sauf que ces dispositions la confirment dans son appréciation que la composition envisagée de trois membres est un non-sens.

Les sanctions

L'article 35 prévoit que la Commission peut prononcer des amendes d'ordre (pouvant aller jusqu'à 10.000.000 de francs pour les personnes morales) ainsi que toute une panoplie de *„sanctions administratives"*, le tout *„sans préjudice des poursuites pénales éventuelles et des peines d'emprisonnement et/ou des amendes prévues par la présente loi"*.

Hormis le fait que le texte ne prévoit aucune voie de recours contre les sanctions administratives et l'amende d'ordre, la Chambre s'interroge, au vu de l'importance de cette dernière, sur l'utilité de pouvoir cumuler les sanctions qui peuvent être prononcées avec celles qui sont du ressort de la justice.

*

LA SURVEILLANCE TOUT COURT ET LA SURVEILLANCE SUR LE LIEU DE TRAVAIL

L'insertion dans le texte des traitements à des fins de surveillance, aussi bien dans la vie quotidienne (article 10) que sur le lieu de travail (article 11), constitue une nouveauté.

Bien que considérés comme pouvant entraîner des atteintes à la vie privée, en combinant différents moyens techniques (images d'une personne reliées à un numéro d'identification), la Chambre estime que ces traitements devraient être réglés par des législations spécifiques. La vidéosurveillance dans le premier cas rentrant plutôt dans le cadre de la prévention et la poursuite d'infractions pénales, une réglementation spécifique des différents cas devrait s'imposer.

La surveillance sur le lieu de travail relève du droit du travail avec ses traits spécifiques. De toute manière, l'article 11 ne précise pas s'il s'applique seulement au secteur privé ou aussi au secteur public, ce qui devrait normalement être le cas dans la logique de non-distinction, mais ce qui se heurte aux obstacles signalés ci-avant sous le titre *„L'application à la fonction publique"*.

En dehors de ces remarques de principe, la Chambre des Fonctionnaires et Employés publics estime que, si surveillance il doit y avoir, celle-ci doit servir à améliorer la protection de l'employé sur des lieux de travail à hauts risques plutôt qu'à surveiller son (in)activité. La Chambre craint en effet que les dispositions du projet, dans leur teneur actuelle, risquent d'être détournées dans le sens des dangers devant lesquels George Orwell nous a mis en garde il y a plus de cinquante ans déjà!

*

L'EXECUTION DE LA LOI

Un aspect très important de toute loi est celui de son application voire de son applicabilité dans la pratique, c'est-à-dire *„sur le terrain"*.

Or, le projet sous avis, surtout mais non seulement en raison de sa technicité très prononcée, risque de poser des problèmes à ce niveau.

En effet, deux aspects supplémentaires sont déterminants à ce sujet.

Il y a en premier lieu la terminologie assez vague qui caractérise certaines dispositions. Ainsi, il est prévu, à l'article 28, que les intéressés ont, entres autres, droit d'accès à leurs données *„à des intervalles raisonnables et sans délais excessifs"*.

Si l'on sait que les procédures mises en place au niveau de la législation sur la comptabilité de l'Etat par exemple ont pour effet que les fournisseurs attendent des mois voire une année pour se voir payés; si l'on sait que la Justice met parfois une décennie à trancher une affaire: comment veut-on alors définir un *„délai excessif"* ou un *„intervalle raisonnable"?*

De même, des termes comme *„données adéquates, pertinentes et non excessives“*, *„certaines données génétiques“*, *„raisons prépondérantes et légitimes“* ou *„sous une forme intelligible“* sont hautement élastiques et n'ont pas leur place dans le texte d'une loi, qui se doit d'être claire et concise. La flexibilité excessive (sic) de la terminologie mise en œuvre ne manquera pas d'insécuriser quiconque se retrouve confronté avec les prescriptions de la loi.

Un autre exemple figure à l'article 6, où il est question de *„données manifestement rendues publiques“*. Dans un monde informatique en permanente évolution, la notion de *„public“* trouve une autre dimension. Les nouveaux moyens de communication permettent la connaissance rapide, sans déplacement et sans grand effort, de certains faits dits *„publics“*.

A titre d'exemple, on peut prendre les registres de population tenus dans les communes. Certaines données de ces registres sont accessibles au public. Les personnes intéressées (huissiers, notaires, etc.) peuvent aller consulter ce registre, soit en se déplaçant, soit par téléphone ou par écrit. Tout en étant publics, ces registres ne sont normalement consultés que par des gens vraiment intéressés. Les nouveaux moyens de communication cependant permettent à tout le monde d'avoir accès à ces registres et ce sans avoir à effectuer un grand effort, sans déplacement etc. On pourra donc consulter ces registres sans être vraiment intéressé, mais par le simple fait qu'on peut y accéder sans difficultés et ce 24 heures sur 24.

Or, le fait de révéler certaines données à différentes personnes n'implique pas nécessairement que l'intéressé ait voulu en informer tout le monde.

En deuxième lieu, il y a le problème – traditionnel – des règlements grand-ducaux d'exécution. Depuis toujours, la Chambre des Fonctionnaires et Employés publics plaide pour l'élaboration de ces règlements en même temps que les lois qui leur servent de base – apparemment sans grand succès.

En effet, le projet de loi sous avis prévoit neuf règlements grand-ducaux d'exécution, dont six qui sont obligatoires et trois qui restent facultatifs. Aucun de ces règlements n'est soumis comme projet à la Chambre, de sorte que le détail des dispositions concernées reste secret. Qui plus est, à défaut de mesures d'exécution, la loi restera inopérante. Tel est notamment le cas en ce qui concerne le règlement grand-ducal dont question à l'article 17, et qui doit autoriser *„les traitements d'ordre général nécessaires à la prévention, à la recherche, à la constatation et à la poursuite des infractions pénales“*. A défaut de ce règlement, la loi restera lettre morte sur ce point!

*

EXAMEN DES ARTICLES

Article 1er

L'article 1er énonce une déclaration d'intention plutôt qu'une disposition légale proprement dite et n'a donc pas sa place dans une loi. La Chambre recommande aux auteurs du projet de maintenir le libellé de l'article 1er de la loi du 31 mars 1979, qu'elle reproduit ci-après et qui résume on ne peut mieux l'objet de la loi:

*„**Art. 1er.** Les personnes physiques ou morales sont protégées contre l'utilisation abusive de données nominatives lors*

a) de la collecte de ces données en vue d'un traitement automatique;

b) de leur enregistrement dans les banques de données;

c) du traitement automatique appliqué à ces données;

d) de la transmission à des tiers de ces données et des résultats de ces traitements.“

Article 2

ad lettre (h)

La définition de la *„surveillance“* d'une personne laisse à désirer alors que la lettre (h) parle d'écrits et de paroles mais reste muette au sujet des images. Traiter un *„mouvement“* ne veut pas nécessairement dire traiter une image, alors que l'utilisation d'une carte magnétique par exemple permet d'enregistrer le mouvement d'une personne dans un bâtiment (accès à différents bureaux etc.) sans que cette personne ne soit *„filmée“*.

Afin d'éviter tout malentendu, il se recommanderait donc de compléter cette disposition en y englobant *„les images“* d'une personne.

Par ailleurs, la définition du terme „*surveillance*“ est particulièrement mal placée sous la lettre (h), les lettres (f) et (g) qui précèdent et (i) et (j) qui suivent concernant respectivement le „*ministre*“, le *„responsable du traitement“*, le *„sous-traitant“* et le *„tiers“*, donc exclusivement des personnes physiques.

ad lettre (k)

La notion *„dans le cadre d'une mission d'enquête particulière“* n'est pas assez précise. Ne faudrait-il pas spécifier *„enquête particulière prévue par une disposition légale ou réglementaire“?*

ad lettre (n)

La page 2 du projet soumis à la Chambre se termine par la lettre (m) alors que la page 3 commence par la lettre (o). Ou bien la lettre (n) a disparu en cours de route, ou bien les lettres (o) à (r) doivent être changées en (n) à (q).

ad lettre (r)

La définition des *„organismes de sécurité sociale“* utilisée par les auteurs du projet englobe les compagnies privées d'assurances, ce qui est évidemment inadmissible.

Article 4

Aux termes du paragraphe (2), une simple autorisation de la Commission suffira pour que les données traitées à des finalités déterminées pourront ultérieurement encore être traitées *„à des fins historiques, statistiques ou scientifiques“*.

La Chambre se demande si on ne devrait pas plutôt prévoir une autorisation légale ou réglementaire à cet effet.

Un autre aspect important, aux yeux de la Chambre, en matière de protection des données, est celui de ce qu'on désigne en allemand par „*Datenvermeidung*“ et „*Datensparsamkeit*“. En effet, des données qui n'existent pas n'ont pas besoin d'être protégées …

La Chambre se demande si l'article 4, qui concerne la *„qualité des données“*, ne devrait pas être complété par l'ajout de ces notions.

Article 7

La Chambre soulève la question de savoir si oui ou non le sous-traitant est soumis au secret professionnel tel que prévu à l'article 458 du Code Pénal, l'article 7 (1) ne parlant que des *„conditions de confidentialité“*.

Article 8

Il n'est question que des condamnations pénales et des jugements civils ou administratifs.

Quid des ordonnances en matière de référé, des jugements et arrêts commerciaux et de ceux rendus par les tribunaux de jeunesse et des tutelles?

Article 18

La Chambre doute que le responsable du traitement soit dans tous les cas en mesure d'apprécier si oui ou non le niveau de protection „*offert*“ par un pays tiers soit suffisant. Le même doute est permis en ce qui concerne cette appréciation par la Commission.

Article 22

Dans le contexte du paragraphe (4) relatif à la *„conservation des preuves“*, la Chambre se permet de rappeler que le droit de la preuve a été modifié par la loi sur le commerce électronique et que, sous certaines conditions, des documents électroniques peuvent valoir à titre de preuve.

Article 23

En ce qui concerne les *„mesures de sécurité particulières“* prévues à l'article 23, la Chambre des Fonctionnaires et Employés publics tient à rendre attentif au fait que le respect des mesures en question

nécessite des investissements humains et financiers considérables. Citons comme exemple l'aménagement des salles d'ordinateurs: ces salles devront être par exemple climatisées et surveillées (éventuellement engagement de personnel) afin d'éviter l'intrusion de personnes non désirées etc.

Article 25

La Chambre est étonnée de constater que la violation des règles relatives à la „*confidentialité*" par exemple est plus sévèrement punie que celle du „*secret professionnel*".

Article 30

Afin d'éviter tout malentendu, il y aurait lieu d'écrire „*3.000.000 LUF*" au lieu de „*3000.000 LUF*" au paragraphe (4).

Dans ce contexte, la Chambre se pose la question de savoir s'il ne valait pas mieux indiquer les amendes et autres montants mentionnés en euros plutôt qu'en LUF.

Article 40

Pour ce qui est du „*chargé de la protection des données*", la Chambre est d'avis que celui ou ceux compétents pour le secteur public devront relever d'un autre statut que ceux du secteur privé.

Quant aux „*assises financières*" de LUF 15.000.000 (!) exigées pour pouvoir être agréé comme chargé de la protection des données, cette condition est foncièrement discriminatoire et de ce fait inacceptable.

Article 41

L'interaction Commission-ILR semble délicate et une attention particulière est à attacher aux dispositions afférentes. C'est pourquoi la Chambre recommande de revoir l'article 41 en collaboration avec les responsables de l'ILR.

*

La Chambre marque son accord de principe quant au fond et aux objectifs déclarés du projet de loi, mais elle exprime les plus graves réserves quant à sa présentation.

Elle s'oppose à la tendance de base, à savoir une espèce d'obstination farouche à forcer les éléments les plus hétéroclites dans un même moule.

Compte tenu de ces observations, la Chambre demande une refonte du texte dans un souci de transparence, de structuration rationnelle et de clarté.

Ainsi délibéré en séance plénière le 22 mai 2001.

Le Secrétaire, *Le Président,*
G. MULLER E. HAAG

Service Central des Imprimés de l'Etat

4735/02

N° 4735[2]

CHAMBRE DES DEPUTES

Session ordinaire 2000-2001

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

AVIS DU PROCUREUR GENERAL D'ETAT

(5.7.2001)

Le présent avis a été élaboré en commun par le Procureur Général d'Etat et les Procureurs d'Etat de Diekirch et de Luxembourg. Il a été rédigé après consultation des Présidents de la Cour supérieure de Justice et des Tribunaux d'arrondissement de Diekirch et de Luxembourg.

Le projet de loi sous rubrique constitue un document d'une grande complexité technique qui soulève toute une série de questions.

Les auteurs de l'avis ont entendu se limiter à examiner les dispositions qui concernent au plus près les attributions des autorités judiciaires, en particulier du Ministère public.

Pour des raisons de présentation, l'avis suivra l'ordre de numérotation des articles du projet de loi, même si certaines dispositions ont une portée plus grande que d'autres.

1) Le traitement de données génétiques (article 6)

L'article 6 (3) règle, entre autres, le traitement des données génétiques qui est interdit, sous réserve des exceptions reprises sous les lettres a-b et les cas visés sub (4) a et b.

L'article 6 (3) exclut du champ des interdictions les traitements lors d'une procédure judiciaire ou d'une enquête pénale. Les données ne peuvent servir qu'à vérifier l'existence d'un lien génétique dans le cadre de l'administration de la preuve en justice, pour la prévention d'un danger concret ou pour la répression d'une infraction déterminée.

A part le fait que la notion d'enquête pénale reste floue (cette remarque vaut également pour d'autres dispositions du projet de loi) et qu'il n'est pas précisé qui est responsable des données, on peut relever que l'objet du traitement, à savoir l'existence d'un lien génétique dans le cadre de l'administration de la preuve en justice est large. Se pose la question de savoir si le terme de procédure judiciaire englobe également les affaires civiles.

Abstraction faite des orientations à prendre dans le cadre de l'élaboration de règles à inclure au Code d'instruction criminelle sur la prise et l'exploitation des échantillons d'ADN, il faut se demander si les dispositions du projet de loi recouvrent toutes les situations qui doivent être envisagées ou qui pourront l'être dans le projet spécifique concernant les analyses d'ADN. Quid du traitement des données aux fins d'identification d'une personne trouvée morte en dehors de toute procédure judiciaire ou d'une enquête pénale? Quid lorsque le traitement concerne non pas un suspect, mais un tiers? Ces situations ne semblent pas permettre un traitement qui rentrerait dans les prévisions de l'article 6 (3).

2) Le traitement de données judiciaires (article 8)

L'article 8 vise les traitements des données dites judiciaires. Cette disposition n'envisage expressément que les données des décisions de justice intervenues en matière pénale, civile ou administrative ainsi que les mesures de sûreté et les sanctions administratives. Il reprend, en cela, à peu près littéralement, les termes de la directive. Ce texte appelle les remarques suivantes:

– Les autorités judiciaires ne sont pas l'auteur de sanctions administratives. Le traitement de ces données est assuré par l'administration auteur de la sanction (sous réserve d'une confirmation par le juge administratif).
– Le concept de mesure de sûreté, repris de la directive, n'est pas des plus clairs en droit luxembourgeois. Si l'on vise par là les décisions en matière de protection de la jeunesse, il serait utile de le préciser. D'autres mesures de sûreté sont prononcées par des décisions de justice et seront dès lors couvertes à ce titre.
– L'article 8 passe sous silence l'ensemble des traitements de données des affaires en cours, en particulier les systèmes informatiques de traitement des affaires pénales (JUPEN), civiles (JUMEE), de blanchiment d'argent (JUOBA), d'entraide judiciaire (RACE), de même que différents systèmes développés et appliqués au niveau des juridictions judiciaires et administratives.
– L'article 8 garde également le silence sur le traitement de données dans le cadre de l'exécution des peines ou de recouvrement des frais de justice.
– L'article 8 impose, pour le traitement de données relatives à des condamnations pénales, l'existence d'une base légale. Le casier judiciaire est certes prévu dans la loi (article 75 de la loi sur l'organisation judiciaire), mais son régime est fixé par un règlement grand-ducal. L'article 8 garde le silence sur les bases juridiques des autres traitements de données, y compris ceux tenus „sous le contrôle de l'autorité publique compétente"; cela signifie-t-il qu'une base réglementaire, du type de celle prévue à l'article 17, n'est pas requise?
– L'article 8 englobe les banques de données judiciaires dans le champ d'application de la loi, y compris pour ce qui est du contrôle effectué par la Commission nationale et l'accès indirect au profit des particuliers. Ce régime n'est pas sans soulever des problèmes pour les banques de données visant des affaires pénales en cours, notamment celles couvertes par le secret de l'instruction au sens de l'article 8 du Code d'instruction criminelle.
– Le „contrôle par l'autorité publique compétente en la matière", dont il est question à l'article 8, soulève des interrogations: Quelle est l'autorité publique visée, les juridictions, les Parquets, le Parquet Général, le Ministère de la justice? Existe-t-il une différence entre la fonction de traitement des données assurée par les autorités judiciaires et la fonction de contrôle? Comment le contrôle dont est investie l'autorité publique compétente s'articule-t-il avec les pouvoirs de contrôle de la Commission nationale?

Les auteurs de l'avis voudraient formuler les propositions suivantes:

– Si le législateur est obligé de reprendre tel quel le libellé de la directive, malgré les imperfections qui le caractérisent, il y aurait lieu, en tout cas, d'ajouter une disposition prévoyant le traitement des données des affaires en cours, contentieuses ou non, des données administratives gérées au niveau des juridictions ou du Ministère public et des données relatives à l'exécution des décisions de justice; cette disposition complémentaire devrait être suffisamment large pour englober toutes les banques de données existantes et susceptibles d'être créées.
– Ainsi qu'il sera précisé par la suite, il y aurait lieu d'inclure les traitements de données résultant d'une surveillance ordonnée par l'autorité judiciaire dans le régime prévu pour les banques de données judiciaires.
– Il faudrait également préciser les responsabilités respectives des autorités judiciaires qui créent et gèrent les traitements en cause et de la Commission nationale. Pour les traitements de données relatives à des affaires en cours, notamment en matière pénale, on peut sérieusement s'interroger sur un contrôle exercé par la Commission nationale et sur un accès indirect au profit des personnes visées.

3) Bases de données de presse (article 9)

Les auteurs de l'avis se sont abstenus de procéder à une analyse détaillée de la problématique inhérente aux traitements de données personnelles à des fins journalistiques, cette question touchant de près la réforme du droit de la presse et la protection des droits des individus. Ils voudraient se limiter, dans le cadre de cet avis, à souligner un problème intimement lié au fonctionnement des bases de données judiciaires.

Est-il acceptable, au regard de la protection des droits individuels, d'établir et d'exploiter, au titre de l'article 8, des bases de données relatives à des affaires judiciaires prescrites ou qui ont été radiées du casier judiciaire à la suite d'une réhabilitation légale ou judiciaire?

4) Traitement à des fins de surveillance (article 10)

Ce texte vise toutes les surveillances effectuées par des entités privées, la police, les autorités judiciaires. Il soulève une série de problèmes:

– Quel régime juridique s'applique à la surveillance en relation avec la sûreté de l'Etat; en d'autres termes, quel est le lien entre les articles 10 et 17 (2)?
– Comment concilier, pour les surveillances ordonnées par les autorités judiciaires, le droit d'information des particuliers et l'accès de la Commission nationale avec le secret inhérent à ces procédures?
– Quels sont, d'une façon plus générale, les liens entre l'article 8 et l'article 10, s'agissant, dans les deux cas, de traitements de données judiciaires?

On peut se demander s'il ne serait pas plus logique d'exclure les surveillances décidées dans le cadre d'une enquête ou instruction du champ d'application de l'article 10 et de les inclure dans un article 8 complété et adapté?

5) Les banques de données „police" (article 17 et 34)

Cette question est particulièrement délicate et les auteurs de l'avis voudraient exprimer leurs réserves fondamentales par rapport au projet de loi.

Sous la loi actuelle du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, la création et l'exploitation de banques de données constituées pour les besoins de la prévention, de la recherche, de la constatation et de la poursuite des infractions, d'ordre général ou particulier, sont réglées par l'article 12-1, introduit dans la loi en 1992 et par le règlement grand-ducal du 2 octobre 1992 relatif à l'exploitation d'une banque de données nominatives de police générale.

Le régime actuel peut être schématisé comme suit:

– Les banques de données en cause relèvent de la police.
– L'enregistrement de certaines données, au titre de conventions internationales ou sur le plan national, ne peut se faire que de l'accord exprès du Procureur d'Etat territorialement compétent.
– Le Procureur d'Etat autorise la transmission de données nationales à Europol.
– La consultation de certaines données est soumise à une information ou à une autorisation préalable du Procureur Général.
– Une autorité de contrôle spécifique, présidée par le Procureur Général ou par son délégué veille au respect des règles d'exploitation de ces banques de données. L'autorité a accès aux banques de données; l'accès de particuliers ne peut se faire que par le biais de cette autorité. Cette autorité de contrôle représente le Luxembourg au sein des autorités de contrôle communes Schengen et Europol.

Le régime actuel est fondé sur une nette distinction entre les compétences de la police, qui est titulaire des banques de données et responsable de leur exploitation, et les compétences du Ministère public qui contrôle le respect des règles d'exploitation.

Il peut être utile d'ajouter que ce régime, fruit de longues réflexions en 1992, a fait ses preuves.

Le projet de loi bouleverse de fond en comble ce mécanisme:

– En vertu de l'article 17, les traitements d'ordre général nécessaires à la prévention, à la recherche, à la constatation et à la poursuite des infractions „réservés" à la Police ou à l'Administration des Douanes et Accises sont autorisés par règlement grand-ducal.
– Le Procureur d'Etat territorialement compétent est „responsable" du traitement.
– La loi de 1979, y compris l'article 12-1, de même que les règlements d'exécution, en particulier le règlement Ingepol de 1992, précité, sont abrogés (article 44); cela signifie que le Procureur Général, agissant en tant que tel ou en tant que président de l'Autorité de contrôle, de même que les Procureurs d'Etat perdent leurs compétences de contrôle.

– Les banques de données police sont traitées comme toute autre banque de données pour ce qui est des pouvoirs de contrôle et d'accès dont sera investie la Commission nationale pour la protection des données.
– Cette Commission représente le Luxembourg dans le cadre des autorités de contrôle communes instituées au niveau international. Relevons que certaines de ces autorités ont un caractère quasi juridictionnel et exigent la participation de délégués nationaux aptes à remplir de telles fonctions.

Le régime proposé dans le projet de loi soulève un nombre d'interrogations très sérieuses:

– Contrairement à ce qui est affirmé dans le commentaire relatif à l'article 17 du projet de loi, ce dernier ne reprend pas la teneur de l'article 12-1 de la loi de 1979, précitée, bien au contraire.
– Quelle sera la responsabilité des Procureurs d'Etat dans les traitements (de données de police) „réservés à la police grand-ducale et à l'Administration des Douanes", alors que les Procureurs d'Etat n'ont aucun pouvoir hiérarchique dans les organes en cause?
– Dans quelle mesure cette responsabilité va-t-elle exposer les Procureurs à un contrôle de la part de la nouvelle Commission nationale? Relevons que l'article 35 investit la Commission nationale du droit de prononcer une sanction d'ordre à l'égard des responsables du traitement. Les Procureurs d'Etat s'exposent-ils à de telles sanctions?
– Comment concilier une telle soumission éventuelle des Procureurs à la Commission nationale avec le mécanisme de recours devant la Chambre du Conseil, régime dans lequel la Commission et le Procureur d'Etat sont investis d'un droit d'action?
– L'assimilation des traitements de données de police à n'importe quelle autre banque de données, au regard de pouvoirs de contrôle et d'accès de la Commission nationale, est-elle compatible avec le caractère particulier de ces fichiers intimement liés aux données traitées dans des affaires judiciaires et éventuellement couvertes par le secret de l'instruction?
– Dans le même ordre d'idées, l'accès indirect au profit des particuliers prévu à l'article 34 du projet de loi, risque d'être incompatible avec les impératifs inhérents aux affaires pénales?
– L'article 17 du projet de loi vise les traitements d'ordre général; sous quel régime seront placées les banques de données „particulières" à certaines affaires pénales ou à un certain type d'infractions?
– Sous le régime actuel, la transmission de données de police nationales à Europol doit être autorisée par le Procureur d'Etat territorialement compétent. Quel sera le mécanisme sous l'égide de la loi nouvelle?
– La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des données des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, que le projet de loi entend transposer en droit luxembourgeois, exclut, expressément, à l'article 3, le traitement des données à caractère personnel mis en oeuvre pour l'exercice, entre autres, des activités de l'Etat relatives à des domaines du droit pénal.

Au regard des difficultés engendrées par le système proposé dans le projet de loi et du champ d'application très clair de la directive, les auteurs de l'avis préconisent le maintien du système actuel prévu par l'article 12-1 de la loi de 1979 et par le règlement lngepol de 1992: Ces textes devraient être adaptés pour tenir compte de la fusion de la police et de la gendarmerie et de l'attribution de certaines compétences de police à l'Administration des Douanes et Accises. Il y aurait également lieu d'étendre le régime de contrôle à toutes les banques de données, y compris celles qui ne sont pas de nature informatique.

A noter que les auteurs du projet de loi No 4794, déposé le 4 mai 2001, portant approbation de la Convention du 26 juillet 1995 sur l'emploi de l'informatique dans le domaine des douanes et de l'Accord relatif à l'application provisoire de cette Convention se placent dans la logique du maintien du régime actuel en se référant expressément à l'article 12-1, paragraphe 4, de la loi de 1979 que le projet actuel entend abroger.

Si l'option d'une suppression du mécanisme actuel devait prévaloir, il faudrait, en tout cas, revoir les attributions du Ministère public. Plutôt que de déclarer les Procureurs d'Etat responsables du traitement de données de police, il faudrait investir ces derniers ou, de préférence, le Procureur Général d'une fonction de contrôle et d'injonction vis-à-vis des titulaires des banques de données. Cette mission de contrôle et d'injonction pourrait déboucher sur une saisine de la Chambre du Conseil. Au niveau des

rapports entre le Procureur et la Commission nationale, il faudrait prévoir que cette dernière ne peut pas agir indépendamment du Procureur Général d'Etat.

6) Le régime de recours (articles 32 et 34 (4 et 5))

L'article 32 introduit le chapitre consacré au recours juridictionnel. Ce texte vise cependant également le „recours devant la Commission". La nature de ce recours n'est pas précisée. Contre quel acte le recours serait-il introduit? Est-ce que l'article 32 vise les saisines et demandes au sens de l'article 34 (4 et 5)? Une demande de vérification n'est pas un recours? L'idée d'un recours devant la Commission nationale accrédite la thèse, qui sera discutée dans la suite, que la Commission nationale est une autorité de nature quasi juridictionnelle.

7) Régime de recours devant la Chambre du Conseil (article 33)

Aux termes de l'article 84 de la Constitution, les contestations qui ont pour objet des droits civils sont exclusivement du ressort des tribunaux. Dans le respect de ce texte, les auteurs de l'avis marquent leur accord avec la proposition de conférer au juge judiciaire la compétence pour statuer sur des demandes de suspension de traitements opérés en violation de la loi.

Le choix de la Chambre du Conseil du Tribunal et de la Cour d'appel est à approuver, au regard d'autres procédures visant des fermetures d'établissement. On peut toutefois s'interroger sur la rigueur des délais qui semblent assez courts, compte tenu de la complexité de la matière.

Il n'y a pas d'inconvénient à investir la Commission nationale d'un droit d'initiative. L'action publique aux fins de condamnation pénale, prévue au point 13 de l'article 33 relèvera, à l'évidence, de la seule compétence du Ministère Public.

Restent quelques interrogations sérieuses:

– Le recours prévu à l'article 33 et la sanction de la fermeture d'établissement s'appliquent-ils à des entités de droit public qui sont responsables de traitement de données en ce compris les organes judiciaires, la police, etc.? En toute logique, la réponse devrait être négative. Le texte du projet de loi ne l'exclut cependant pas expressément.
– La combinaison des articles 17 et 33 soulève un problème dans la mesure où le Procureur d'Etat est à la fois „responsable" du traitement des données de police et investi du droit d'agir en cas de violation des conditions légales.
– Un autre problème concerne les pouvoirs de contrôle de la Chambre du Conseil sur le respect, par l'autorité judiciaire dont relève cette même chambre du Conseil, des règles régissant les traitements de données judiciaires.
– Il faut relever, pour terminer, des incohérences certaines au niveau des peines spécifiques prévues dans les différents articles. Saute aux yeux, notamment, la divergence entre la peine prévue à l'article 33 (13), en cas de manquement à une ordonnance de la Chambre du Conseil, à savoir 3 millions LUF, et la sanction administrative prononcée par la Commission nationale au titre de l'article 35, à savoir 10 millions LUF.

8) Attributions de la Commission nationale (articles 34 et 35)

Les articles 34 et 35 figurent également parmi les dispositions qui suscitent de la part des auteurs du présent avis des réserves.

– Les articles 34 et 35 investissent la Commission nationale de pouvoirs très importants exercés au titre de fonctions fondamentalement différentes. La Commission est à la fois instance de contrôle, instance d'investigation à l'instar d'un juge d'instruction, instance de recours, instance de coopération avec des autorités étrangères et instance de sanction.

  Le cumul de ces fonctions de nature à la fois administrative et juridictionnelle, qui vont bien au-delà de ce qui est prévu dans la directive, soulève des interrogations en ce qui concerne le principe de la séparation des pouvoirs et la protection des droits de l'individu.
– Parmi les différentes fonctions de la Commission, celle de prononcer des sanctions (voir article 35) est particulièrement sujette à caution. Ce régime de sanction s'applique-t-il indifféremment aux

entités de droit privé et aux entités de droit public? Les organes du pouvoir judiciaire pourront-ils faire l'objet de sanctions administratives pour les banques de données qu'elles entretiennent; quid d'administrations comme la police ou les contributions? Si les entités de droit public sont exclues, il faudrait le préciser.

– Les amendes dites d'ordre prévues dans ce texte sont à qualifier de sanctions pénales au sens de la Convention européenne des droits de l'homme. La compatibilité de ce régime de sanctions administratives avec les dispositions constitutionnelles nationales et conventionnelles sur la protection des droits de l'homme en matière pénale n'est pas évidente. A noter, en particulier, que la règle fondamentale de la légalité des délits et des peines, qui exige une détermination précise de l'infraction et de la peine, n'est pas respectée.
– L'articulation entre le régime de sanction dite administrative et les sanctions prononcées par les juridictions au titre de l'article 33 n'est pas claire.
– Quelles sont les voies de droit ouvertes contre une décision de la Commission nationale? La directive exige, expressément, à l'article 28 (3), que les décisions de l'autorité de contrôle peuvent faire l'objet d'un contrôle juridictionnel. En toute logique, la personne lésée devrait pouvoir saisir le juge administratif. Le projet de loi ne le précise toutefois pas. De quel type de recours s'agira-t-il, recours en annulation ou recours en réformation? Comment les compétences du juge administratif pourront-elles s'articuler avec celles du juge judiciaire? Quid en cas de divergence de décisions intervenues dans le cadre des procédures de l'article 33 et de l'article 35?
– Il faut relever que, au niveau du pouvoir de sanction de la Commission nationale, le projet de loi va, une fois de plus, beaucoup plus loin que la directive. Celle-ci prévoit, à l'article 28 (3), des pouvoirs d'investigation et d'intervention pour les autorités nationales. La sanction se résume à un avertissement ou à une admonestation. Pour le surplus, la directive prévoit que l'autorité nationale saisit le juge.
– Au regard du texte de la directive, on peut s'interroger sur la compatibilité du système prévu par le projet de loi avec le droit communautaire. Le projet de loi transforme une autorité de contrôle en autorité quasi juridictionnelle investie d'un important pouvoir de sanction.

Les auteurs du présent avis considèrent qu'il y a lieu de réserver le pouvoir de prononcer des amendes aux juridictions et de limiter les attributions de la Commission aux mesures prévues à l'article 28 de la directive.

Le système à mettre en place pourrait être conçu de la façon suivante: La Commission, à l'issue d'un contrôle, adresse un avertissement ou une admonestation au responsable du traitement, l'invitant ainsi à se mettre en conformité avec la réglementation. Si le responsable n'obtempère pas, il y a lieu de prévoir la possibilité d'une saisine des juridictions pénales compétentes. Ce mécanisme implique que le non-respect des règles légales critiqué dans l'avertissement ou l'admonestation est érigé en infraction. La Commission nationale pourra soit se borner à dénoncer cette infraction aux autorités judiciaires, comme il est dit à l'article 34 (7), soit être investie d'un droit d'action au sens de l'article 33 (1) du projet de loi. Une saisine parallèle des juridictions administratives peut ainsi être évitée, la démarche de la Commission s'inscrivant dans une logique de contrôle et de répression de nature pénale assurant toutes les garanties juridictionnelles aux concernés.

9) Dispositions spécifiques (article 41)

L'article 41 prévoit un régime particulier d'accès aux données concernant les abonnés des opérateurs de télécommunication et/ou des services postaux et/ou des fournisseurs de services.

Ce texte vise indifféremment les autorités déterminées aux articles 88-1 à 88-4 du Code d'instruction criminelle, le Procureur d'Etat et toute personne agissant dans le cadre de la sauvegarde de la vie humaine.

Outre le fait que la notion de sauvegarde de la vie humaine n'est pas autrement précisée, on peut s'interroger sur la légitimité d'une assimilation des différentes hypothèses envisagées par le projet de loi.

Les compétences des autorités judiciaires, Procureur en cas de flagrant délit ou juge d'instruction, en relation avec les articles 88-1 à 88-4 du Code d'instruction criminelle sont à discuter dans le cadre d'une

réforme éventuelle des dispositions pertinentes du Code d'instruction criminelle et ne sauraient faire l'objet de dispositions dans des lois particulières réglant des matières techniques.

Luxembourg le 5 juillet 2001.

Pour le Procureur Général d'Etat,

Georges WIVENES

Avocat général

Service Central des Imprimés de l'Etat

4735/04

N° 4735[4]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

AVIS DE LA CHAMBRE DES EMPLOYES PRIVES

(30.10.2001)

Par lettre du 15 décembre 2000, Monsieur François Biltgen, Ministre délégué aux Communications, a soumis le projet de loi No 4735, réf. B5807, sous rubrique à l'avis de la Chambre des Employés Privés.

*

I. REMARQUES PRELIMINAIRES

Une réforme qui s'imposait

1. Le projet de loi soumis a l'ambition de réglementer le traitement des données à caractère personnel tout en cherchant à équilibrer la protection des droits privés et des droits fondamentaux avec la liberté de circulation des données. Jusqu'à présent, cette matière était régie par la loi du 31 mars 1979 (adaptée à plusieurs reprises) réglementant l'utilisation des données nominatives dans les traitements informatiques. Cette loi répondait aux exigences d'une époque au cours de laquelle le traitement informatique se limitait à l'existence d'un nombre réduit de banques de données, souvent étatiques.

De nos jours, le progrès informatique fait rage et l'exigence que la création d'une banque de données devrait être soumise à l'autorisation préalable du ministère compétent (article 4 de la loi de 1979) est tout simplement devenue illusoire. Le traitement de données à caractère personnel n'est plus un domaine essentiellement réservé à l'Etat. Il est tout à fait juste d'affirmer que la démocratisation de l'outil informatique, l'accroissement de la vitesse de traitement de l'information, ainsi que l'accroissement des capacités de stockage et des capacités de communication ont causé l'obsolescence de la loi du 31 mars 1979.

Cette loi est donc dépassée par le progrès technologique qui s'est produit au cours des vingt dernières années. La transposition de la directive 95/46/CE permet non seulement d'harmoniser les lois nationales des Etats membres mais également de moderniser la loi luxembourgeoise en cette matière.

2. La transposition en droit national aurait dû s'opérer dans un délai de trois ans à compter de son adoption par le Parlement européen, c'est-à-dire pour le 24 octobre 1998 au plus tard! Malgré le retard important du Grand-Duché, la Chambre des Employés Privés accueille positivement la volonté du Gouvernement d'adapter, enfin, la législation en cette matière aux exigences d'aujourd'hui.

3. Adapter la législation aux exigences actuelles signifie également tenir compte du passage de la monnaie nationale à l'euro à partir de l'an prochain. La Chambre déplore que les amendes pénales prévues dans le texte soient encore libellées en francs et non pas en euros.

4. La CEP•L est consciente du fait qu'une protection des données ne peut jamais être absolue. Le présent projet de loi doit par conséquent se limiter à la tentative de protéger de la meilleure façon qui

soit les droits privés ainsi que les droits fondamentaux en matière de protection des données personnelles.

5. En comparant le texte de la directive avec celui du projet de loi soumis, il est à remarquer que le texte national dépasse, à certains endroits la directive européenne dans sa rigueur face à la protection des droits des particuliers.

6. Malgré ces efforts, le texte du projet de loi reste assez vague et imprécis, laissant la fixation des détails aux soins des tribunaux et de la Commission nationale de protection des données.

7. La CEP•L tient à remarquer que la lecture du texte du projet est compliquée par un nombre exagéré de renvois qui rendent la compréhension inutilement difficile. Dans un souci d'une meilleure compréhension, il serait souhaitable que le texte de la future loi qui résultera de ce projet adopte la technique rédactionnelle législative que l'on retrouve généralement dans les textes de loi.

8. L'innovation la plus importante du projet de loi soumis se produit, aux yeux de la Chambre des Employés Privés, au niveau de la surveillance sur le lieu de travail. C'est pour cette raison que nous y avons consacré la part prépondérante de notre avis. Une autre partie comporte des remarques ponctuelles sur certains articles du projet de loi.

*

II. LA SURVEILLANCE SUR LE LIEU DE TRAVAIL (articles 10 et 11)

Afin de pouvoir apprécier l'étendue de la nouvelle loi, il faut prendre en considération le régime et la réalité actuels qui règnent dans les sociétés.

Aujourd'hui, le contrôle de l'employeur des activités de ses salariés pourrait être absolu!

9. Nombreuses sont les sociétés où les employés utilisent un badge d'accès: ainsi l'employeur peut toujours analyser le temps de travail de chacun de ses employés. En outre, dans de nombreuses sociétés, le réseau informatique permet à l'employeur de regarder à tout moment le travail que l'employé est en train de réaliser sur son ordinateur.

L'ordinateur, le badge d'accès, le téléphone, etc. sont des outils qui n'ont pas été spécialement conçus pour collecter des données personnelles sur les salariés d'une entreprise, mais qui sont pourtant susceptibles d'être exploités à cette fin. Il s'agit justement d'éviter de telles pratiques.

10. La Chambre des Employés Privés accueille favorablement la volonté du Gouvernement de construire une base légale du traitement des données à des fins de surveillance sur le lieu de travail. Jusqu'à présent ce domaine se caractérise avant tout par un vide juridique pouvant donner lieu à de sérieux abus. Aujourd'hui, en cas d'accord de l'employé, l'employeur a le droit de collecter de telles données. Or, il est fort possible que le consentement donné par l'employé, limité dans sa décision par l'existence du lien de subordination existant entre lui et son patron, soit en réalité beaucoup moins volontaire qu'il l'affirme. Il faudrait empêcher les employeurs d'abuser du lien de subordination dont ils disposent à l'égard de leurs employés pour en profiter d'imposer des méthodes de surveillance inappropriées.

L'article 11 du projet de loi relatif au traitement de données à des fins de surveillance sur le lieu de travail

11. Contrairement à la directive 95/46/CE, relative à la protection des données à caractère personnel, qui ne traite pas particulièrement cette question, l'article 11 du projet de loi se consacre entièrement au traitement de ces données qui ont été collectées dans un but de surveillance sur le lieu de travail.

Le traitement de données à des fins de surveillance sur le lieu de travail est limité à quatre cas précis:

- la sécurité et la santé des travailleurs;
- la protection des biens de l'entreprise;

- le contrôle du processus de production portant uniquement sur des machines;
- le contrôle temporaire de la production ou des prestations du travailleur en vue de mesurer son activité permettant de déterminer sa rémunération.

12. Il s'agit en fait d'une copie de la convention collective No 68 conclue le 16 juin 1998 par le Conseil national du travail belge stipulant les conditions d'autorisation de la surveillance par caméras sur le lieu de travail.

Le présent projet de loi reprend donc ce texte pour l'appliquer non seulement à la surveillance par caméra, mais à tout traitement de données à des fins de surveillance sur le lieu de travail.

13. La convention collective belge prévoit en outre que s'il „apparaît que la surveillance peut avoir des implications sur la vie privée d'un ou de plusieurs travailleurs, il appartiendra au conseil d'entreprise ou, à défaut, au comité pour la prévention et la protection du travail d'examiner les mesures à prendre pour réduire l'ingérence dans la vie privée à un minimum".

Le projet de loi luxembourgeois n'accepte ce droit d'intervention du comité mixte d'entreprise que lorsque le traitement de données dans l'entreprise se fait pour des besoins de sécurité, ainsi que pour le contrôle temporaire de production ou des prestations du travailleur en vue de mesurer son activité afin de déterminer sa rémunération.

En d'autres termes, si l'employeur arrive à justifier que le traitement de données se fait dans le but de protéger les biens de l'entreprise ou de contrôler le processus de production des machines, il le pourra librement et sans devoir en rendre compte à son personnel. Il est seulement tenu d'informer les personnes concernées.

Il n'existe alors aucun moyen de contrôle de la part des représentants du personnel que le traitement se fait uniquement dans ces objectifs. Des abus de la part de l'employeur sont alors possibles.

Le consentement de l'employé

14. Le présent projet de loi entend combattre de telles pratiques abusives en stipulant qu'un tel contrôle ne peut être que temporaire et avoir pour objectifs d'assurer la sécurité et la santé des travailleurs et de vérifier la production ou les prestations du travailleur en vue de mesurer son activité afin de déterminer sa rémunération.

L'article 11 stipule que „le consentement exprès de la personne concernée ne rend pas légitime le traitement mis en oeuvre par l'employeur".

Une telle surveillance doit obtenir l'accord préalable de la Commission nationale pour la protection des données dont la décision est subordonnée à l'avis préalable de l'Inspection du Travail et des Mines. Enfin l'employeur, sous peine de poursuite pénale, doit informer la personne concernée, ainsi que les représentants du personnel ou à défaut l'ITM de la finalité du traitement, de la ou des périodes de surveillance, de la durée et le cas échéant des conditions de conservation des données.

Toutes ces mesures ont pour but d'éviter la commission d'abus par l'employeur dans le traitement des données.

15. Notons encore à ce sujet que la loi espagnole engage l'*Agencia de Proteccion de Datos* à informer les citoyens de leurs droits dans le cadre du traitement automatique des données à caractère personnel. A ce sujet, elle a mené des campagnes de sensibilisation en 1999. En outre, cette *Agencia* donne des conseils personnalisés dans ses bureaux. On pourrait s'imaginer que la Commission Nationale pour la Protection des Données se dote de missions similaires.

Ce n'est pas le contrôle en lui-même qui est mis en cause

16. Il découle du lien de subordination de l'employé par rapport à son patron que ce dernier surveille le travail de ses salariés. Mais il existe une marge entre la surveillance des employés et le recensement systématique de toute information sur les employés susceptible d'intéresser l'employeur. Une telle pratique est contraire aux droits individuels et est donc à éviter.

17. Il importe donc de déterminer les motifs pour lesquels l'employeur collecte ses informations. Toute la problématique du traitement de données sur le lieu de travail joue autour de sa finalité. Si elles

ont été collectées dans le but d'assurer le bon fonctionnement de l'entreprise, respectivement la protection contre des intrusions extérieures, le traitement de ces données est légitime. Par contre, si elles ont été recueillies avec pour objectif d'assurer un contrôle continue sur les employés, le traitement est à éviter.

18. Il s'agit dorénavant de trouver un équilibre entre la possibilité de surveillance des employés et le respect de leurs libertés et droits fondamentaux. En fixant plusieurs conditions, dont notamment l'exigence de l'autorisation préalable de la Commission nationale pour la protection des données, le projet de loi cherche à établir cet équilibre.

Le texte du projet de loi confère à la Commission nationale pour la protection des données, à l'Inspection du Travail et des Mines, ainsi qu'aux représentations de personnel la lourde responsabilité de surveiller les employeurs afin d'éviter que des abus ne soient commis. Le bon traitement des données à caractère personnel sera en fin de compte déterminé en fonction de la rigidité du contrôle effectué par ces organismes sur les employeurs.

Toutefois, un certain nombre de questions à régler ne sont pas soulevées dans ce projet de loi. De quelles possibilités de contrôle sur la finalité du traitement disposent les représentants du personnel? Quels sont leurs moyens d'action en cas d'abus de l'employeur? Toutes ces précisions font malheureusement défaut dans le texte du projet de loi. La Chambre des Employés Privés estime que le présent projet devrait contenir des dispositions réglant les moyens d'action des délégations de personnel, respectivement, des comités mixtes d'entreprises en cas de détournement de finalité des données par l'employeur.

19. En outre, la Chambre des Employés Privés revendique que la problématique du traitement des données à des fins de surveillance sur le lieu de travail fasse partie de la panoplie des dispositions (cf. loi PAN du 12 février 1999) qui devront obligatoirement être prévues entre les parties dans les conventions collectives de travail.

*

III. REMARQUES PONCTUELLES CONCERNANT LE PROJET DE LOI

Un plus du projet de loi: protection des données des personnes morales et inclusion de l'élément génétique

20. L'objet du projet de loi, présenté dans le premier article, est la défense de la vie privée ainsi que des libertés et des droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel. En outre, le projet entend faire respecter les intérêts légalement protégés des personnes morales. Par ce dernier élément, le projet dépasse le cadre des dispositions prévues dans la directive 95/46/CE, qui ne contient aucune disposition relative aux personnes morales.

Contrairement à la directive, le projet de loi inclut encore l'élément génétique dans la notion de données à caractère personnel. La protection des données génétiques sera probablement le défi le plus important de demain en matière de protection de données informatiques.

La CEP•L félicite le Gouvernement d'avoir introduit ces deux notions dans le projet de loi.

Le traitement „ultérieur" des données: une notion vague

21. L'article 4 (1) (a) stipule que le responsable du traitement doit garantir que les données sont collectées pour des finalités déterminées, explicites et légitimes, et ne seront pas traitées *ultérieurement* de manière incompatible avec ces finalités.

22. L'article 4 (2) dispose que les données traitées à des finalités déterminées peuvent être traitées *ultérieurement* à des fins historiques, statistiques ou scientifiques dans les conditions prévues par le régime d'autorisation préalable de la Commission.

Deux observations sont à faire:

- Le terme „ultérieurement" est assez vague pour le traitement de ces données à des fins historiques, statistiques ou scientifiques. D'un point de vue temporel, „ultérieurement" peut être immédiatement ou quelques dizaines d'années après la collecte de la donnée. Une précision s'impose donc.

- Même si le traitement des données à ces finalités est soumis à l'autorisation préalable de la Commission, la CEP•L est d'avis que cette mesure n'est pas suffisante pour garantir le respect des droits privés.

  Qu'en est-il du droit à l'information qui, d'après le projet de loi, doit se faire au plus tard au moment de la collecte de la donnée? La simple information au moment de la collecte du genre „le signataire accepte de mettre ses données personnelles au service d'éventuelles études historiques, statistiques ou scientifiques ultérieures" ne peut être considérée comme suffisante.

  Qu'en est-il du droit d'opposition du concerné? En effet, pour pouvoir s'y opposer, encore faudrait-il qu'il en soit informé.

Le traitement de catégories particulières de données

23. L'article 6 du projet de loi interdit le traitement de données révélant l'origine raciale, ethnique, les opinions politiques, les convictions religieuses et philosophiques, l'appartenance syndicale, ainsi que celui relatif à la santé, à la vie sexuelle et aux données génétiques.

La volonté du Gouvernement d'interdire ce genre de traitement serait fort attrayante, si cet article ne contenait pas huit exceptions (par exemple sauf exceptions le consentement de la personne concernée, ou encore, un motif d'intérêt public important), auxquelles s'ajoutent encore quelques exceptions qui sont propres à l'interdiction du traitement des données génétiques. D'autres paragraphes portant sur des exceptions contiennent elles-mêmes des exceptions.

La Chambre des Employés Privés déplore le fait que dans cet article, qui protège les droits individuels, ce soit l'exception qui fasse la règle.

La notion de l'indisponibilité du corps humain

24. Le traitement des données à caractère personnel n'est plus interdit lorsque le concerné donne son consentement, sauf indisponibilité du corps humain et sauf les cas où l'interdiction ne peut être levée par le consentement de la personne concernée.

25. La notion de l'indisponibilité du corps humain peut donner droit à des interprétations des plus fantaisistes. Même si dans l'exposé des motifs, l'auteur affirme que cette notion „appréhende et prohibe les comportements déviants tels l'eugénisme ou la reproduction cellulaire aboutissant au clonage", chaque responsable de traitement de données pourra en établir sa propre interprétation. Il est dommage que le texte du projet ne soit pas plus explicite afin de pouvoir éviter certains abus d'interprétation.

Le traitement de catégories particulières de données par les services de la santé

26. L'article 7 lève l'interdiction prévue dans l'article 6 lorsque le traitement est nécessaire, entre autres, aux fins de la médecine préventive, des diagnostics médicaux et aux fins de la recherche scientifique dans le domaine de la biologie et de la médecine. La seule condition prévue est l'obtention de l'autorisation de la Commission nationale pour la protection des données.

27. L'article 7 pose la problématique du clonage. Bien qu'il soit indirectement interdit par l'article 6 (2) (a), qui traite de l'indisponibilité du corps humain, qui rappelons-le est une notion équivoque, les défenseurs de la recherche en matière de clonage justifient leur position en invoquant notamment que cette recherche serait utile dans la lutte contre les maladies, respectivement dans la prévention des maladies.

Ce projet de loi pourrait ouvrir la porte au clonage des cellules humaines. Une telle recherche est rendue possible, sous condition de l'accord préalable de la Commission nationale pour la protection des données. La CEP•L est d'avis qu'une décision d'une telle importance devrait être prise par une représentation nationale et non pas par un organisme purement administratif.

L'autorisation préalable de la Commission pour l'interconnexion de données

28. L'autorisation préalable ne pose aucun problème lorsque le traitement des données se fait exclusivement sur le territoire du Grand-Duché. Mais on voit mal une société multinationale qui dispose

d'une filiale dans notre pays demander une telle autorisation à la Commission nationale de protection des données luxembourgeoise. Il est douteux que cet article soit vraiment praticable dans la réalité.

L'autorisation par voie réglementaire

29. L'autorisation par voie réglementaire:

- lève l'interdiction du traitement de données qui révèlent l'origine raciale ethnique, les opinions politiques, les convictions religieuses et philosophiques, l'appartenance syndicale, ainsi que le traitement de données relatives à la santé, la vie sexuelle et les données génétiques (article 6h);
- permet le traitement à des fins de surveillance prévu par l'article 10, sans avoir à respecter les conditions énumérées;
- libère le responsable du traitement de l'obligation préalable de notification à la Commission prévue par l'article 12.

L'autorisation par voie réglementaire est délivrée pour les traitements de données effectuées en cas d'enquêtes de fraude menées par la police et l'administration des douanes et accises. Le règlement grand-ducal établi à cet effet détermine le procureur responsable du traitement ainsi que les données sur les personnes concernées, la finalité du traitement, etc.

30. Notre Chambre se demande pourquoi un règlement grand-ducal et non pas un acte délivré par une juridiction d'instruction procure cette autorisation de traitement de données? Le règlement grand-ducal sera forcément établi sur ordre d'un ministre, qui pourrait donc ordonner des enquêtes policières comme bon lui semble et sans devoir se soumettre à un contrôle.

La CEP•L est d'avis que la Commission nationale de protection des données, liée par le secret professionnel, devrait être informée, au moins a posteriori, sur le traitement de données qui a été effectué par les forces de l'ordre sur telle ou telle personne. Il est primordial pour un Etat de droit qu'un organe indépendant puisse apprécier le traitement de ces données, afin d'éviter que des abus se produisent.

Le transfert de données vers des pays tiers

31. En vertu de l'article 18, les transferts de données dans des pays non membres de l'Union européenne ne sont autorisés que si le pays en question en assure un niveau de protection adéquat.

Quels sont les critères d'un niveau de protection adéquat? Au moins aussi bien qu'en Union européenne ou mieux ou moins bien et dans quelles limites? Qui contrôle ce caractère adéquat?

32. Ne serait-il pas mieux que la Commission dresse une liste des pays dont les mesures sont adéquates et une liste de ceux dont les mesures ne sont pas adéquates et que cette liste soit constamment tenue à jour?

Exceptions au droit à l'information de la personne concernée: l'intérêt économique ou financier important

33. Le point (e) de l'article 27 prévoit que le droit à l'information de la personne concernée ne s'applique pas en présence d'un intérêt économique ou financier important de l'Etat ou de l'Union européenne, en particulier dans les domaines monétaire, budgétaire et fiscal.

Notre Chambre voit mal quels seraient ces intérêts économiques (dont la définition fait d'ailleurs défaut) qui permettraient de bafouer les droits et libertés fondamentales pour raison financière de l'Etat ou de l'Union européenne.

Recours devant la Chambre du Conseil: des audiences non publiques

34. La CEP•L accueille le fait, qu'en raison de leur caractère personnel des données traitées, les audiences de la Chambre du conseil de la Cour d'Appel ne soient pas publiques (article 33 point 9). Toutefois la répartition des compétences entre la Commission et de la Chambre du Conseil ne ressort pas clairement du projet de loi.

35. Ainsi une personne, qui estime qu'un traitement de données la concernant s'est opéré de manière illégitime, peut s'adresser simultanément à la Commission nationale pour la protection des données et à la Chambre du conseil de la Cour d'appel (article 32 du projet de loi).

Deux organismes différents, l'un purement administratif, l'autre juridictionnel, sont donc susceptibles de se pencher en même temps sur le même dossier et risquent d'adopter des positions opposées! Il se pourrait que la Commission nationale considère que le litige en question ne nécessite pas une action en justice, alors que la Chambre du Conseil, quant à elle, estime que le responsable du traitement devrait être condamné pour son comportement irrégulier.

36. Comme les jugements de la Chambre du Conseil sont susceptibles d'un recours, la Commission, en tant que défenseur de l'intérêt de la présente loi, pourrait même faire appel contre une décision de cette juridiction qui a tranché en faveur d'un particulier et contre une administration. La raison d'être de la Commission, à savoir la défense des libertés et droits fondamentaux en matière de traitement des données à caractère personnel, serait alors anéantie.

Dispositions spécifiques: la sauvegarde de la vie humaine

37. L'article 41 permet à toute personne agissant dans le cadre de la sauvegarde de la vie humaine, d'accéder de plein droit sur requête et par l'intermédiaire de l'Institut de régulation (ILR) aux données concernant les abonnés des opérateurs de télécommunications.

38. Bien que l'état d'urgence exige que l'aidant puisse accéder dans certains cas aux données d'un abonné de téléphone, la Chambre des employés privés voit mal pourquoi cette possibilité soit ouverte à „toute personne" comme il est marqué dans le projet de loi. Ne serait-il pas suffisant que seuls les services de secours disposent de ce moyen?

39. Sous réserve des observations faites plus haut, la Chambre des Employés Privés marque son accord au présent projet de loi.

Luxembourg, le 30 octobre 2001.

Pour la Chambre des Employés Privés,

Le Directeur,
Théo WILTGEN

Le Président,
Jos KRATOCHWIL

Service Central des Imprimés de l'Etat

4735/03

N° 4735[3]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

AVIS DE LA CHAMBRE DE TRAVAIL

(14.11.2001)

Par lettre en date du 15 décembre 2000, référence B58071, notre chambre a été saisie pour avis du projet de loi No 4735 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel.

Notre chambre soucieuse de la protection des personnes à l'égard des données à caractère personnel se doit de formuler des remarques tant d'ordre général que ponctuel.

*

I. OBSERVATIONS GENERALES

A. Le projet de loi ne risque-t-il pas d'entraver les droits fondamentaux de la personne?

Le considérant 3 de la directive 95/46/CE dispose que *„l'établissement et le fonctionnement du marché intérieur dans lequel, conformément à l'article 7A du traité, la libre circulation des marchandises, des personnes, des services et des capitaux est assurée, nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un Etat membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés"*.

La directive cherche donc à trouver un équilibre entre la libre circulation des marchandises (données) et la protection des droits fondamentaux de la personne à l'égard de ces données.

Force est cependant de constater que cet „équilibre" se fait au détriment des derniers si l'on se réfère à l'article 1 alinéa 2 de la directive qui dispose que *„les Etats membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre Etats membres pour des raisons relatives à la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée"*.

Cet article n'est que la consécration des articles 28 et 29 du traité de Rome, garants de la libre circulation des marchandises.

Voilà pourquoi le message donné par la Commission européenne est clair: la libre circulation des données prime la protection des personnes à l'égard du traitement des données à caractère personnel.

Le projet de loi a-t-il pour autant repris la philosophie de la directive?

A priori, le lecteur pourrait croire le contraire en lisant l'article 1 qui ne se réfère plus au concept de la libre circulation des marchandises mais uniquement à la protection des droits fondamentaux de la personne.

Les bonnes intentions ne perdurent cependant pas si l'on analyse la suite des articles ainsi que l'exposé des motifs du projet de loi lequel illustre de façon éloquente l'approche de la Commission européenne. Voici quelques passages évocateurs:

„La Commission européenne présenta un paquet de mesures, dont l'objet était d'harmoniser dans les Etats membres de l'Union européenne les législations en matière de protection des données, afin

que celles-ci ne soient plus à l'origine de restrictions ou d'interdictions à la libre circulation des données à caractère personnel dans le marché unique …"

L'harmonisation des législations des Etats membres en matière de protection des données n'est pas une fin en soi, mais un moyen pour promouvoir le marché intérieur.

Voilà pourquoi il est évident que la protection des personnes à l'égard du traitement des données à caractère personnel ne peut être que minimaliste comme le laisse sous-entendre le passage suivant de l'exposé des motifs:

„Le principe de la libre circulation des données est reconnu dans la directive 95/46/CE. Ceci implique nécessairement que l'on passe d'un système d'autorisation préalable à un système de plus grande liberté dans lequel l'autorisation préalable serait réduite à la portion congrue …

La libre circulation des données est un corollaire nécessaire à la liberté du commerce et de l'industrie …

La libre circulation des données est d'autant plus importante que la dimension du Grand-Duché de Luxembourg, sa place financière exigent une facilitation et une accélération des flux de données avec un niveau de sécurité juridique accru."

Notre chambre ne peut, au vu des considérations formulées ci-dessus, partager l'opinion que le projet de loi établit un équilibre entre les intérêts du marché intérieur et la protection des personnes à l'égard des données à caractère personnel.

Elle se permet davantage de démontrer dans l'analyse des articles que les droits fondamentaux de la personne ont été réduits au plus petit dénominateur commun.

B. Légiférer au compte-gouttes accentue davantage l'arbitraire!

Notre chambre conteste catégoriquement la façon de procéder du gouvernement qui consiste à se référer à d'innombrables reprises à des règlements d'application qui pourtant font défaut au moment de la saisine de notre chambre. Ceci va davantage accroître l'arbitraire et l'incohérence en la matière:

– d'abord, dans la mesure où un texte de loi est difficilement applicable si les règlements grand-ducaux auxquels il renvoie n'ont pas encore été élaborés;
– puis, dans la mesure où, à un moment ultérieur, les acteurs de la procédure législative sont obligés de relire le texte de loi ainsi que leurs avis y relatifs pour apprécier la légalité des règlements grand-ducaux.

C. Le projet de loi, un texte indigeste truffé d'exceptions!

Bien que le texte du projet ne fasse plus référence au principe de la libre circulation des marchandises tel qu'évoqué dans la directive, il prévoit dans presque tous les articles tant de dérogations ou de tempéraments à la conception restrictive du traitement des données à caractère personnel que l'on peut avoir l'impression que le principe devient exception et vice versa.

Pour ne citer qu'à titre d'exemple les articles 6 et 7 du projet ayant trait au traitement de catégories particulières de données respectivement au traitement de catégories particulières de données par les services de la santé.

Le paragraphe 1 de l'article 6 établit le principe d'interdiction des données dites sensibles.

Le paragraphe 2 énumère les exceptions qui sont bel et bien au nombre de huit.

L'article 7 continue dans le même flou artistique en prévoyant dans son paragraphe 1 – hormis les exceptions prévues au paragraphe 2 de l'article 6 – une exception supplémentaire au principe d'interdiction de traitement des données dites sensibles de l'article 6 paragraphe 1.

Le paragraphe 2 de l'article 7 prévoit pour le traitement de catégories particulières de données par les services de la santé une autorisation préalable de la Commission.

Le paragraphe 3 du même article prévoit de nouveau des dérogations où pour certains traitements il suffit d'une simple notification.

Le paragraphe 4 de l'article 7 va encore plus loin dans la mesure où un règlement grand-ducal permet de déroger à l'interdiction du traitement de données sensibles lorsqu'il s'agit de les communiquer à des tiers ou de les utiliser à des fins de recherche.

Ici on ouvre encore davantage la brèche aux abus dans la mesure où la loi accorde à un règlement le pouvoir de déroger à ses propres principes et dérogations.

La question épineuse reste de savoir si l'article 7 paragraphe 4 constitue une dérogation aux dérogations des articles 6 et 7 ou bien une dérogation aux principes des articles 6 et 7.

Cette façon de légiférer est inacceptable pour notre chambre. Elle érige en principes les exceptions, et ceci bien évidemment, au détriment de la protection des droits fondamentaux de la personne.

*

II. ANALYSE DES ARTICLES

Deux principes sacro-saints constituent la trame du présent projet, d'une part, le principe de la finalité du traitement des données personnelles et d'autre part, le principe de proportionnalité du traitement des données personnelles.

Le premier principe repose sur le postulat que la menace pour la vie privée que constituent les traitements de données à caractère personnel réside davantage dans la finalité qu'ils poursuivent que dans la nature des données traitées.

Le second précise que les données doivent être nécessaires, et non seulement utiles, pour qu'un traitement puisse être accompli. Ce principe vise l'évaluation de l'opportunité d'introduire une donnée à caractère personnel dans un traitement par rapport à la finalité de ce traitement.

C'est au sujet de ces deux principes, qui constituent le fil conducteur du projet, que notre chambre a le plus de réserves à faire.

Elle va l'illustrer par la suite dans l'analyse des articles.

Ad article 5 Légitimité du traitement

L'article 5 prévoit différentes conditions, en application desquelles un traitement portant sur des données à caractère personnel est considéré comme légitime.

Comme les conditions de légitimité sont alternatives et non pas cumulatives, il se peut très bien qu'un traitement remplisse la condition (a), mais pose des problèmes au niveau de la condition (d).

On pourrait ainsi imaginer que, par exemple, des écoutes téléphoniques soient légitimes sur base de la condition (a), parce qu'il existe des dispositions légales permettant sous certaines conditions de recourir à ces mesures alors qu'elles ne le seraient pas au vu de la condition (d), parce que les droits et libertés fondamentaux de la personne suspectée et de ses concitoyens seraient lésés, notamment lorsque la mesure est disproportionnée par rapport au but poursuivi ou excède la finalité initiale pour laquelle elle a été prévue.

Dans le cas d'espèce, il pourrait y avoir un conflit entre deux conditions qui sont susceptibles de s'appliquer toutes les deux, sachant toutefois qu'elles sont alternatives.

Cela voudrait-il dire que la Commission nationale de la protection des données pourrait se baser sur la condition (a) pour éviter l'application de la condition (d) ou vice versa.

Notre chambre est d'avis que si plusieurs conditions peuvent s'appliquer simultanément à une situation donnée, il faudra évaluer les différentes conditions entre elles. S'il se révélait qu'en vertu du principe de finalité ou de proportionnalité, le traitement excéderait sa finalité ou serait disproportionné, il devrait être interdit.

Ainsi, si dans notre cas une disposition légale prévoit de recourir sous certaines conditions aux écoutes téléphoniques, il doit rester possible de l'écarter s'il se révèle qu'elle ne remplit pas les critères de finalité et de proportionnalité tels que prévus aux articles 4 paragraphe 1 (b) et 5 paragraphe 1 (d).

Ad article 6 Traitement de catégories particulières de données (données sensibles)

A l'instar de ce qui a été dit en introduction, il est légitime de se poser la question si l'interdiction de traitement des données dites sensibles constitue le principe, eu égard à la multitude d'exceptions prévues par ce même article.

Tout en étant conscient que le décryptage du génome humain peut être bénéfique pour la société, notre chambre tient néanmoins à remarquer que le traitement ou la transmission de données génétiques

peut aussi être utilisé à d'autres fins, notamment dans le secteur des assurances et des relations de travail entre employeur et salarié afin de n'assurer respectivement n'embaucher que les personnes qui, du point de vue génétique, ne sont pas susceptibles d'être affectées par certaines maladies, plus ou moins graves. Le risque d'une stratification de la société en deux classes, les „génétiquement sains", d'une part et les „génétiquement affectés", d'autre part existe bel et bien.

Qu'arrive-t-il si le salarié ou l'assuré ont donné leur consentement exprès à un tel traitement pour conclure un contrat de travail ou un contrat d'assurance et si la loi n'interdit pas la levée de l'interdiction du traitement des données génétiques?

Le risque est grand que, vu la subordination ou la faiblesse économique du salarié resp. de l'assuré à l'égard de l'employeur resp. de l'assureur qui lui demandent la communication de ses données génétiques, le premier, sous l'effet de l'ignorance et de l'intimidation, donne *nolens volens* son consentement à un tel traitement.

Est-on encore en présence d'un consentement libre et éclairé si la personne en question n'a aucune alternative pour refuser un tel traitement de ses données?

Ad article 10 „Traitement à des fins de surveillance"

Le paragraphe 1 (b) est en somme le reflet de ce que l'auteur essaie d'éviter, à savoir le phénomène „Big brother's watching you".

Notre chambre est d'avis que ce phénomène existe bel et bien déjà et quiconque peut s'apercevoir de l'installation de vidéocaméras installées aux abords des routes ou au centre-ville.

Le paragraphe précité est conçu en des termes si flous et généraux qu'un traitement à des fins de surveillance est possible dans „tout lieu accessible ou non au public (…), pourvu qu'il présente (…) un risque rendant le traitement nécessaire à la prévention, la recherche, la constatation et la poursuite d'infractions pénales".

Ce paragraphe en permettant donc aux autorités d'installer des vidéocaméras un peu partout, comme bon leur semble est contraire au critère de „prévisibilité".

Etant donné que la délinquance au sens large est omniprésente non seulement dans les agglomérations, mais également dans les localités de la campagne (surtout les vols avec effraction), il faudrait donc étendre le dispositif des vidéocaméras à l'entièreté du territoire luxembourgeois si l'on ne veut pas se laisser faire le reproche qu'une infraction commise en province mérite moins d'attention (de surveillance) que dans les centres-villes.

Cette politique a posteriori de surveillance renforcée montre que la mise en oeuvre de l'ouverture des frontières internes de l'Union européenne a entraîné des inconvénients dont on ne pouvait, dès le début, mesurer l'ampleur.

Pour détecter les auteurs d'infractions, les autorités luxembourgeoises sont contraintes de surveiller un peu n'importe qui et n'importe où. Est-il alors exagéré de prétendre que les droits et libertés individuelles des personnes sont réduits à une portion congrue?

Notre chambre a de sérieux doutes que même une prolifération des moyens de surveillance sur tout le territoire – parce que les infractions sont commises un peu partout – réduise de façon considérable le nombre d'infractions. Pour lutter contre la délinquance et la criminalité, l'auteur du projet est prêt à prendre en ôtage (surveiller) la société tout entière. Cette façon de procéder ne peut être acceptée par notre chambre. Elle est plutôt d'avis qu'il faudrait davantage investir dans la formation de la police, dans les réseaux de police interétatiques (Europol) et de doter ceux-ci des moyens en personnel et en matériel nécessaires plutôt que de chercher une solution de facilité – une surveillance renforcée par caméras – qui se fait, d'ores et déjà, au détriment des libertés individuelles des personnes.

Notre chambre n'analyse qu'en ordre subsidiaire le paragraphe 2 qui prévoit que „les personnes concernées sont informées par des moyens appropriés tels que des panneaux de signalisation, des circulaires (…)".

A ce sujet, elle se doit cependant de constater qu'en pratique, tel n'est souvent pas le cas.

Il n'y a pas de signalisation informant le citoyen que des vidéocaméras sont installées aux abords des routes ou à l'intérieur des tunnels, comme il n'y en a pas pour les vidéocaméras installées (et dissimulées) à l'extérieur des établissements financiers et scolaires.

D'ailleurs qu'est-ce que l'auteur entend par „personnes concernées"?

Les personnes concernées ne sont pas seulement les personnes suspectées, mais également toutes les autres personnes qui se font capter contre leur gré, faute de signalisation, par une caméra.

Dans un ordre très subsidiaire, et pour autant que le traitement à des fins de surveillance soit indispensable, quod non, notre chambre est d'avis que la signalisation de vidéocaméras pourrait décourager bon nombre de délinquants potentiels à commettre des infractions, parce qu'ils n'oseraient pas exécuter leurs projets s'ils savaient que leurs actes seraient enregistrés et pourraient le cas échéant, valoir comme moyen de preuve en justice.

Ad article 11 Traitement à des fins de surveillance sur le lieu de travail

Par nature, la caméra constitue un moyen excessivement disproportionné au but recherché par l'employeur, qu'il s'agisse de la discipline, de l'amélioration de la productivité, de la sécurité ou encore de la lutte contre les vols. L'enregistrement continu des faits et gestes du salarié dans son activité professionnelle permet, en effet, de mettre en évidence des éléments qui ne relèvent pas de la sphère professionnelle, mais ressortent de la personnalité, de l'identité de l'individu.

A ce sujet il y a lieu de se référer à un passage d'un article du „Monde diplomatique" (août 1999) dont la teneur est la suivante:

> „(…) Une étude menée en 1998 par l'American Management Association sur mille quatre-vingt-cinq firmes, montre ainsi que 40% des entreprises sont engagées dans une forme de surveillance intrusive de leurs employés. Elles vérifient les courriers électroniques, les conversations téléphoniques, le contenu des boîtes vocales, saisissent les mots de passe des ordinateurs individuels, enregistrent sur vidéo numérique les performances de travail. Le contrôle aléatoire de la présence de drogue dans le sang est le fait de 41% des entreprises américaines, tandis que 15% pratiquent des tests psychologiques cherchant à connaître les pensées intimes et les attitudes."

Notre chambre craint fort que de telles pratiques n'existent également au Luxembourg. Bien que la volonté du Gouvernement de légiférer en la matière soit en elle-même louable, mais qu'il existe un risque permanent de violation des droits fondamentaux dans la mise en oeuvre des moyens de surveillance, la loi sert donc tout au plus à légaliser ces pratiques, inconnues du public.

Voilà pourquoi notre chambre est d'avis que les principes de finalité et de proportionnalité des traitements des données personnelles étaient déjà voués à l'échec avant qu'ils n'eussent vu le jour.

Même si un traitement à des fins de surveillance sur le lieu de travail se révélait indispensable, quod non, il serait *ab initio* impossible de l'instaurer pour une finalité limitée et déterminée, parce que le captage des images sur le lieu de travail contient inévitablement des éléments liés à l'intimitée de la vie privée de chacun des travailleurs, éléments qui pourtant n'entrent pas dans la finalité initiale de la surveillance. L'impossibilité de limiter par nature la finalité du traitement entraîne par essence la disproportionnalité de cette mesure.

Ainsi, le captage ou l'enregistrement d'images des travailleurs sur le lieu de travail n'entrant pas dans la finalité prévue par la loi pourraient servir comme moyen de preuve à une autre fin ou finalité.

Il se pourrait que dans le cadre de la surveillance à des fins de sécurité, une attitude ou un acte d'un salarié qui ne rentrent pas dans le champ d'application de la finalité prévue par la loi soient utilisés ultérieurement à une autre fin, par exemple, comme moyen de preuve servant à justifier un licenciement.

Il s'agit de savoir si l'employeur peut faire valoir ce moyen de preuve illicite – car son utilisation est destinée à une finalité différente de celle prévue par la loi – pour licencier ce salarié. Le juge va-t-il admettre ce moyen de preuve en vertu du fait que „la fin justifie les moyens" ou bien va-t-il rejeter ce moyen de preuve pour cause de détournement de sa finalité?

Notre chambre s'oppose énergiquement à l'introduction de tout genre de moyens de surveillance, électroniques ou numériques, ayant pour but „le contrôle temporaire de production ou des prestations du travailleur en vue de mesurer son activité afin de déterminer sa rémunération".

Ce contrôle va rejeter le travailleur dont l'émancipation a été le fruit d'âpres luttes syndicales au terreau du prolétariat réifié du dix-neuvième siècle. Le travailleur devient de nouveau matière fongible, taillable et corvéable à merci pour les employeurs.

Dans un ordre très subsidiaire, et pour autant qu'un traitement à des fins de surveillance soit indispensable, notre chambre demande que le comité mixte d'entreprise doive pouvoir décider non seulement dans les cas visés aux lettres (a) et (d), mais également dans les cas visés aux lettres (b) et (d),

ceci conformément à la procédure qui est prévue à l'article 16 de la loi du 6 mai 1974 instituant des comités mixtes dans les entreprises. Par ailleurs elle demande d'accorder le même pouvoir de décision aux délégués du personnel, si le comité mixte d'entreprise fait défaut.

Cet article est le corollaire de l'article 15 de la directive qui flanque le principe de protection de l'individu à l'égard de décisions individuelles automatisées prévu au paragraphe 1 de deux exceptions qui annihilent le principe prévu au paragraphe 1.

En fait cela veut dire que si l'employeur propose au salarié au moment de la conclusion ou de l'exécution de son contrat de travail de se soumettre à un traitement à des fins de surveillance, le salarié ne peut refuser cette mesure en pratique, malgré le principe évoqué à l'article 15 paragraphe 1, s'il ne veut pas risquer de perdre son travail. Bel exemple que pratique et théorie divergent fondamentalement!

Ad article 14 „Autorisation préalable de la Commission"

Le problème est que, si une telle autorisation n'est pas demandée par le responsable du traitement ou lui est refusée et qu'il utilise ou transmet, malgré tout, des données sensibles à un tiers, les sanctions pénales prévues au paragraphe 3 de cet article ne sauraient tout de même réparer le préjudice subi par la personne qui a fait l'objet du traitement.

Toujours est-il qu'une personne tierce en possession de données personnelles peut, à son tour, de nouveau communiquer celles-ci à une autre personne. Bref, la transmission de données personnelles par le biais de plusieurs responsables de traitement ne peut être effacée *ab initio*.

Concernant le paragraphe 2, notre chambre se demande si l'Inspection du travail et des mines dont l'avis préalable doit être demandé en vue de l'autorisation préalable de la Commission n'a pas un conflit d'intérêts dans la mesure où d'une part, de par la loi du 4 avril 1974 portant réorganisation de l'ITM, elle a pour mission de veiller au respect des conditions de travail des travailleurs, de la sécurité et de la santé au travail et d'autre part, de par la présente loi, elle est obligée de donner son avis sur les conditions de travail (au sens large) dont elle doit elle-même assurer le contrôle.

Ad article 17 „Autorisation par voie réglementaire"

Notre chambre – à l'instar de ce qu'elle a déjà soulevé en introduction – s'oppose énergiquement à la façon de procéder de l'auteur qui se contente de régler le domaine du droit pénal ainsi que de la sûreté de l'Etat et de la sécurité publique par voie réglementaire, ceci pour deux raisons:

d'abord, parce que ces dispositions – d'autant plus qu'elles sont susceptibles d'affecter davantage les droits fondamentaux de la personne – devraient être intégrées dans la présente loi pour éviter que le gouvernement puisse à sa guise se tailler un règlement sur mesure, modifiable à tout moment, qui ne nécessite pas l'approbation du parlement;

et

puis, afin que notre chambre puisse en connaissance de cause évaluer le bien-fondé de ces dispositions par rapport aux autres dispositions du projet de loi et de la directive.

Ad article 18 „Principes" dans le cadre des transferts de données vers des pays tiers

Notre chambre juge inacceptable que le texte laisse l'appréciation „du niveau adéquat de protection du pays tiers" au responsable du traitement qui, dans bien souvent des cas, a des intérêts propres dans un tel transfert. Il serait donc à la fois juge et partie.

Par ailleurs le texte ne précise nulle part ce qu'il entend par „un niveau de protection adéquat".

Notre chambre est d'avis que le responsable du traitement doit saisir la Commission nationale de la protection des données du moment qu'il envisage de transférer des données à un pays tiers et que cette dernière doit établir des critères pour définir „le niveau de protection adéquat".

Elle ne voit pas pourquoi le texte envisage la saisine de trois acteurs différents (responsable du traitement, en cas de doute de ce dernier, la Commission nationale, en cas de doute de cette dernière, la Commission européenne) pour juger le cas échéant du „niveau adéquat de protection du pays tiers". Tout cela est bien peu transparent!

En effet notre chambre se demande de quelle protection bénéficie la personne concernée si le responsable a transféré des données à un pays tiers dont le niveau de protection n'est pas „adéquat".

Ad article 19 „Dérogations“

L’article 19 est tout à fait caractéristique pour tout le projet.

Il ajoute de l’arbitraire à l’arbitraire.

Cette obsession de flanquer chaque article d’une panoplie d’exceptions et de renvois rend le texte illisible, incompréhensible et partant inapplicable.

Le paragraphe 2 qui prévoit que „dans le cas d’un transfert effectué vers un pays tiers n’assurant pas un niveau de protection adéquat, le responsable du traitement doit notifier à la Commission un rapport établissant les conditions dans lesquelles il a opéré le transfert“ constitue, selon notre chambre, une mesure tardive et inutile, car le transfert a déjà eu lieu et un dommage peut déjà s’être produit. On ne peut plus retourner en arrière pour effacer le transfert de traitement.

Le paragraphe 3 prévoit qu’un tel transfert peut être autorisé par la Commission même si le pays tiers n’assure pas un niveau de protection adéquat à la condition que le responsable assure des garanties suffisantes au regard de la protection des droits fondamentaux de la personne. Notre chambre doute fort que la personne concernée soit en mesure d’évaluer le bien-fondé de ces garanties afin de donner son consentement „éclairé“ en toute liberté, ceci d’autant plus que le responsable du traitement a lui-même souvent des intérêts propres financiers dans un tel transfert.

La personne concernée, qui est également la partie la plus faible du point de vue économique, risque fort d’être dupée.

Ad article 21 Confidentialité des traitements

Notre chambre a de sérieux doutes qu’une manipulation, une altération ou un détournement de traitement de données ne puissent pas se faire par autrui sans l’autorisation du responsable du traitement.

Voilà pourquoi elle se demande si, et dans quelles hypothèses, la partie cocontractuelle du responsable du traitement agit vraiment „sous l’autorité du responsable du traitement“.

A contrario, se pose-t-elle la question ce qu’il advient lorsqu’une personne n’agit pas sous l’autorité du responsable?

Ad article 22 Sécurité des traitements et ad article 23 Mesures particulières de sécurité

L’article montre bien que la sécurité des traitements qui incombe au responsable n’est qu’une obligation de moyens et non de résultat.

Ceci veut dire concrètement que si la personne subit un préjudice suite à une destruction, perte, altération ou diffusion de ses données, elle ne peut engager la responsabilité de l’auteur du traitement que si elle prouve une faute dans le chef de l’auteur du traitement alors que dans le cas où il se serait agi d’une obligation de résultat, la responsabilité de l’auteur du traitement aurait été établie d’office, à moins qu’il n’arrivât à s’exonérer en prouvant un cas de force majeure.

Cette atténuation de protection pour la personne concernée montre bel et bien qu’il n’existe pas de sécurité absolue en matière de traitement de données, et que tout orfèvre en la matière, que tout internaute expérimenté est en mesure de surpasser les garde-fous dans ce domaine.

Nul n’ignore que le système Echelon des Etats-Unis est apte à espionner de manière routinière téléphone, fax et courrier électronique dans le monde entier.

Compte tenu de cette réalité, n’est-il pas un peu osé de la part des législateurs européen et national de donner au citoyen l’impression qu’un maximum de sécurité est garanti pour protéger les droits fondamentaux de la vie privée des personnes?

Chacun sait que les obligations énumérées à l’article 23 pour assurer la sécurité des traitements ne peuvent être respectées toutes en même temps.

Il est donc illusoire de promettre un maximum de sécurité du traitement des données aux personnes concernées.

Ad article 26 Le droit à l’information de la personne concernée

Notre chambre se doit de constater qu’en pratique ce droit à l’information de la personne concernée est souvent bafoué.

Un article du Monde diplomatique de mai 2000 intitulé „Soupçons sur les banques d'ADN" confirme que, surtout dans le domaine de la génomique, les violations du droit à l'information de la personne concernée sont très fréquentes.

En l'espèce, une fondation pour la recherche se lance dans la collecte d'ADN de Français âgés de plus de 90 ans, afin de mettre en évidence les mécanismes génétiques de la longévité, c'est-à-dire, les gènes dont la présence assurerait une protection naturelle contre les maladies.

A cette fin, la fondation a constitué une banque de données génétiques. A l'insu de l'initiateur et des personnes concernées de ce projet, la direction de la fondation a signé un contrat avec une société de biotechnologie sur la banque de données génétiques dans lequel la fondation touchait, en contrepartie du droit exclusif accordé à cette société à valoriser les résultats de la banque, une contribution financière de 32 millions de FF.

Souvent il arrive que, comme en l'espèce, le responsable du traitement n'est pas le responsable ou représentant de l'entreprise qui, contre le gré du premier, passe outre à la procédure d'information.

Vu l'enjeu financier dans les transferts de données génétiques, il n'est pas étonnant que certains avares n'ont pas les moindres scrupules pour se passer du droit à l'information de la personne concernée.

Le plus gênant dans les contrats qui se passent entre laboratoires publics et sociétés privées, c'est qu'ils consentent pour la plupart une exclusivité au payeur sur la banque de données ADN. C'est contre l'intérêt des malades, puisque cela exclut toutes les autres pistes de recherche qui pourraient être menées à partir de cette banque, avec d'autres partenaires.

Voilà pourquoi notre chambre émet ses plus grandes réserves que de telles dispositions puissent empêcher des dérives telles que décrites ci-dessus.

Ad article 27 Exceptions au droit à l'information de la personne concernée

Notre chambre est d'avis que les dérogations à l'article 26 mettent en cause le principe même du droit à l'information de la personne concernée, ceci surtout dans des cas où le justiciable est exposé à des enregistrements d'entretiens téléphoniques, de décryptage des mots de passe etc.

Même dans des domaines comme la sûreté de l'Etat, de la défense, de la sécurité publique et de la recherche d'infractions, notre chambre juge indispensable que la personne suspectée dispose au moins *a posteriori* d'un droit à l'information et au contenu des traitements opérés par les responsables.

Ce droit à l'information est encore plus important si la personne lésée entend attaquer un tel traitement de données en justice. A défaut d'obligation d'informer le justiciable, tout recours contre un tel traitement est voué à l'échec *ab initio.*

Philippe Rivière dans un article du Monde diplomatique, édition mars 1999, confirme les objections formulées par notre chambre en écrivant à ce sujet:

> *S'il est logique de requérir que „la cible" ne soit pas avertie des modifications (des traitements) effectuées pour exécuter l'ordre d'interception, il est en revanche, plus inquiétant de constater que les opérateurs seront tenus de protéger les informations qu'ils détiennent sur la nature et le nombre des interceptions en cours ou réalisées et de ne pas divulguer les informations liées à la méthode d'interception. Qui, en ce cas, pourrait rendre compte des activités de surveillance?*

Ad articles 28 et 29 sur le droit d'accès et ses exceptions

Mêmes remarques que pour les articles 26 et 27.

L'article 29 ne précise pas dans quels cas le droit d'accès est limité et dans quels autres il est différé. Qu'en est-il par exemple en cas d'écoutes téléphoniques?

La distinction est importante dans la mesure où dans le premier cas il y a une restriction quant à l'accès des données alors que dans le deuxième cas il y a un report dans le temps du droit d'accès.

Comme le responsable doit motiver la limitation ou le report dans le temps du droit d'accès, notre chambre demande qu'il doive motiver sa décision *in concreto* et qu'il ne suffise pas d'indiquer un motif *in abstracto* (p.ex. la recherche d'infractions).

Contrairement au paragraphe (4) in fine, notre chambre est d'avis que la Commission *doit* communiquer à la personne concernée le résultat de ses investigations, *y compris leur contenu*.

Ad article 30 Droit d'opposition de la personne concernée

Notre chambre se demande comment une personne peut faire opposition contre un traitement dont elle n'a pas connaissance.

Le problème majeur est que, dans la plupart des cas, la personne concernée ignore complètement que des données personnelles le concernant soient traitées.

Ad article 31 Décisions individuelles automatisées

Ce droit de ne pas se soumettre à une décision individuelle automatisée se révèle souvent illusoire.

Y a-t-il des salariés qui oseront s'opposer – même en présence d'un motif raisonnable et légitime – à une telle décision d'un employeur? La conséquence de l'exercice d'un tel droit par le salarié serait probablement qu'il mettrait en péril sa relation de travail.

Ad article 34 Missions et pouvoirs de la Commission Nationale pour la Protection des Données

Notre chambre se demande si, conformément au paragraphe 3(e), la Commission a été préalablement consultée à l'adoption de ce projet de loi et, si dans l'affirmative, pourquoi il n'a pas été annexé au présent projet de loi.

Ad article 36 Composition de la Commission Nationale pour la Protection des Données

En vue de mieux protéger les intérêts des citoyens – en leur qualité de travailleur et de consommateur, notre chambre exige que les organisations syndicales les plus représentatives au niveau national soient également représentées dans la Commission.

Ad article 41 Dispositions spécifiques

Notre chambre tient à préciser que les articles 88-1 à 88-4 du code d'instruction criminelle ne couvrent pas tous les moyens techniques de surveillance et de contrôle.

Les écoutes téléphoniques étant un de ces moyens, il y a lieu de préciser qu'il existe trois types d'écoutes, à savoir les écoutes judiciaires (articles 88-1 et 88-2), les écoutes administratives (articles 88-3 et 88-4) et les écoutes dites sauvages.

Concernant les écoutes judiciaires, notre chambre réfute que cette procédure initialement prévue pour détecter les personnes suspectées de terrorisme et de trafic de drogues soit ouverte à la poursuite de presque toute infraction. Dans les faits, tout juge peut demander à écouter n'importe qui. Il suffit de préciser que c'est pour la bonne cause.

Ceci est d'autant plus contestable que l'écoute judiciaire est absolument indétectable. Impossible donc, pour un particulier de savoir qu'il est écouté.

Les mêmes remarques valent également pour les écoutes administratives qui peuvent être ordonnées par le Premier Ministre aux fins de rechercher des infractions contre la sûreté extérieure de l'Etat que un ou plusieurs auteurs tentent de commettre, ou ont commises ou tenté de commettre.

En pratique cependant, il existe un autre moyen de surveillance non prévu par la loi, à savoir les écoutes sauvages. Ces écoutes téléphoniques sont effectuées sans aucun mandat officiel. Contraires aux lois sur le respect de la vie privée, ces écoutes sont souvent utilisées dans des affaires d'espionnage industriel ou, plus prosaïquement, dans des histoires de divorce.

*

CONCLUSION

Compte tenu des remarques formulées précédemment prouvant à suffisance de droit que les principes de proportionnalité et de finalité de la loi sont voués à l'échec ab initio, notre chambre estime que le projet de loi soulèvera plus de problèmes qu'il n'en résoudra.

Nul n'ignore qu'il peut faire l'objet d'une mesure de surveillance sans qu'il s'en aperçoive, à quelque titre que ce soit. Après les attentats terroristes du 11 septembre 2001 au WTC à New-York et au Pentagone à Washington, cette crainte semble davantage justifiée, comme le témoignent par exemple les projets de mesures que le gouvernement allemand entend mettre en oeuvre sous le prétexte du terrorisme („Rasterfahndung", empreinte digitale de tous les citoyens …).

Rien ne permet de penser que les pratiques de contrôle et de surveillance ayant existé jusqu'à ce jour, en l'absence d'un texte juridique, vont cesser dès l'entrée en vigueur de la présente loi. Certaines pratiques ne sont même pas couvertes par elle comme l'espionnage économique et militaire.

Par ailleurs l'efficacité d'une telle législation est limitée dans la mesure où elle ne couvre que l'espace économique européen, à l'exclusion du reste du monde. Ceci n'empêche donc pas les mesures de surveillance et de contrôle en Europe à partir de pays tiers.

Au lieu de réduire le contentieux en la matière, notre chambre craint que le présent projet de loi n'aggrave l'engorgement des tribunaux. Dans une telle hypothèse, il serait tout à fait incertain et aléatoire comment les tribunaux appliqueraient le principe de proportionnalité en tenant compte des libertés individuelles, d'une part et de l'intérêt collectif, d'autre part.

Finalement notre chambre craint que l'imagination de quelques-uns pour épuiser les lacunes de la loi ne puisse l'emporter sur sa finalité. Si tel était le cas, la loi manquerait son but!

Voilà pourquoi notre chambre a le regret de vous informer qu'elle marque son désaccord avec le présent projet de loi, ceci tant quant au fond que quant à la forme.

Veuillez agréer, Monsieur le Ministre, l'expression de nos sentiments très distingués.

Luxembourg, le 14 novembre 2001.

Le Directeur,
Marcel DETAILLE

Le Président,
Henri BOSSI

Service Central des Imprimés de l'Etat

4735/05

N° 4735[5]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

AVIS DE LA CHAMBRE DES METIERS

(22.11.2001)

Par sa lettre du 15 décembre 2000, Monsieur le Ministre délégué aux Communications a bien voulu demander l'avis de la Chambre des Métiers au sujet du projet de loi repris sous rubrique.

Le projet de loi a, d'une part, pour objectif de réagir face aux progrès techniques et aux possibilités offertes par les nouvelles technologies de l'information et, d'autre part, de transposer en droit national 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 la libre circulation de ces données.

Il entend abroger la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, devenue vétuste avec le développement technologique et qui de ce fait n'est en large partie plus appliquée.

*

1. OBSERVATIONS GENERALES

1.1. L'importance de „l'information" au niveau de la gestion de l'entreprise

Pour exercer leurs activités économiques et afin de se positionner dans un environnement concurrentiel en évolution rapide, les entreprises ont besoin d'un nombre toujours croissant d'informations nominatives.

Ainsi les traitements de données personnelles sont-ils indispensables à la gestion des principales fonctions de l'entreprise: ressources humaines, gestion des rémunérations, sécurité (contrôle de l'accès aux locaux, vidéosurveillance), suivi de la clientèle (comptes-clients, service après-vente, mailings, établissement de profils-clients), marketing, prospection commerciale etc.

Par conséquent, les entreprises entretiennent souvent plusieurs banques de données nominatives.

Avec l'émergence de la société de l'information depuis le milieu des années 90, les informations en provenance de sources diverses stockées sur support informatique sont devenues un facteur de production de première importance, qui est commercialisé au même titre que les facteurs travail et capital.

L'importance des données informatiques est telle que de véritables marchés de données se sont créés. Cette évolution s'est intensifiée au cours des dernières années avec le développement fulgurant d'Internet.

En effet, dans un monde économique où le service au client gagne de plus en plus d'importance et où le positionnement correct sur le marché devient la seule chance de survie pour bon nombre d'entreprises, la connaissance du comportement du marché joue un rôle plus que jamais prépondérant.

La primauté des informations sur le marché et la clientèle est telle que souvent des bases de données font partie intégrante du fonds de commerce de nombreuses entreprises. Etant donné que, eu égard aux conditions de marché souvent difficiles, les petites et moyennes entreprises affichent un besoin réel en données sur leur entourage – notamment leurs clients –, la Chambre des Métiers considère que l'utilisa-

tion des données informatiques doit être facilitée le plus possible tout en instituant des mesures adéquates de protection des droits et libertés fondamentaux.

Le Parlement Européen et le Conseil de l'Union Européenne considèrent dans la Directive 95/46/CE que „les systèmes de traitement de données (…) doivent respecter les libertés et droits fondamentaux des personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus". La Directive précise par ailleurs que „l'établissement et le fonctionnement du marché intérieur (…) nécessitent non seulement que les données à caractère personnel puissent circuler librement d'un Etat membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés".

Cet aspect est d'autant plus important qu'une partie considérable de la vie économique va se dérouler par l'intermédiaire de réseaux informatiques, et les flux d'informations automatiquement générés suite à l'interconnexion entre plusieurs ordinateurs gagneront de plus en plus d'importance pour les entreprises.

C'est pour cette raison, que de l'avis de la Chambre des Métiers, la Directive évoque au même titre aussi bien la nécessité de la protection des droits fondamentaux des personnes en relation avec le traitement informatique de données personnelles que l'importance de ces données pour le développement économique.

La Chambre des Métiers ne peut que se rallier à ces considérations en soulignant que la réalisation d'un de ces objectifs ne peut se faire aux dépens de la réalisation de l'autre.

1.2. Les changements en perspective pour les entreprises

Avec l'adoption du nouveau projet de loi, des modifications significatives sont apportées par rapport au régime en vigueur actuellement.

Il y a tout d'abord lieu de noter que, contrairement à la loi de 1979, qui s'appliquait aux seules bases de données informatisées, le projet de loi étend indistinctement la protection au traitement informatisé et à la tenue d'un fichier manuel. Il en résulte que dorénavant plus de traitements informatisés entrent dans le champ d'application de la loi.

Un changement majeur par rapport à la loi de 1979 consiste dans l'introduction du principe de la notification du traitement informatique avec contrôle a posteriori, le principe de l'autorisation préalable restant seulement applicable dans les cas où le traitement présente un risque intrinsèque d'atteinte au respect de la vie privée, au regard de la nature des données traitées et de la finalité du traitement (p. ex. le traitement concernant les données génétiques …).

La Chambre des Métiers peut être d'accord avec une telle approche dans la mesure où elle simplifie les formalités préalables de mise en oeuvre des traitements de données personnelles les plus banals tout en maintenant un cadre réglementaire plus strict entraînant une protection de la vie privée, susceptible d'être atteinte par certains types de traitements informatiques.

La Chambre des Métiers propose de prévoir la possibilité d'une notification par voie électronique.

Le projet de loi introduit par ailleurs plusieurs principes novateurs qui guident la protection des personnes à l'égard des traitements de données les concernant.

Il s'agit du „principe de la qualité des données" (principes de loyauté, de finalité, de mise à jour et de limitation de la durée de conservation des données) et du „principe de la légitimation des données", qui forment ensemble ce qu'il convient d'appeler les conditions générales de licéité des traitements.

Le principe de finalité du traitement s'avère être le fil conducteur du projet de loi. Ainsi, la finalité doit être définie par les entreprises antérieurement à la mise en oeuvre du traitement. C'est elle qui justifie la collecte et qui limite le champ de l'utilisation des données collectées. Elle doit être connue de la personne concernée et une fois réalisée, les données collectées doivent être détruites.

Il s'agit aux yeux de la Chambre des Métiers d'un bon critère dans la mesure où il ne risque pas d'être dépassé par la technologie.

Contrairement à la loi de 1979, le projet de loi énumère les cas dans lesquels les données à caractère personnel peuvent faire l'objet d'un traitement par les entreprises. Ainsi, un traitement informatique qui n'est pas repris sur la liste ne peut pas être autorisé. En revanche un traitement, même s'il y est énuméré, ne peut être mis en ceuvre qu'à la condition de respecter les conditions générales de licéité.

A côté des principes à respecter par les entreprises dans la mise en oeuvre d'un traitement, le projet de loi attribue plusieurs droits aux personnes concernées par la collecte de données informatiques. En plus du droit à l'information et du droit d'accès, qui existaient déjà sous la loi de 1979, le projet de loi institue un droit nouveau, à savoir le droit d'opposition. Il permet à toute personne de s'opposer au traitement de certaines données pour des raisons prépondérantes et légitimes tenant à sa situation particulière. L'objectif de ces dispositions en faveur des personnes concernées est de responsabiliser davantage celui qui traite des données à caractère personnel.

Le projet de loi, censé concilier l'impératif de la libre circulation des données et l'impératif de la protection des droits et libertés, impose également de nombreuses obligations aux entreprises. Tout traitement de données, quelle que soit son importance, tombe dans le champ d'application de la nouvelle loi.

L'intégration par les entreprises de ces principes dans leurs stratégies informatiques constitue dès lors une charge administrative importante et implique de profonds changements en termes d'organisation, et ce plus particulièrement pour les petites et moyennes entreprises.

La Chambre des Métiers entend observer que ce carcan de règles assez étroit n'arrivera très probablement pas à cerner le vrai danger en matière de protection des droits et libertés fondamentaux, qui, au stade actuel des évolutions sur les marchés internationaux, ne vient pas des petites et moyennes entreprises, mais plutôt des grandes entreprises, souvent établies à l'étranger. A défaut de la fixation de règles dans le cadre d'accords multilatéraux, une protection efficace et complète ne pourra pas être atteinte.

La Chambre des Métiers peut toutefois être d'accord avec le cadre général tracé par le projet de loi dans la mesure où il est de nature à sécuriser les entreprises et les consommateurs dans le nouveau contexte de la société de l'information et des opportunités offertes par le commerce électronique. Il vient utilement compléter le dispositif de sécurité mis en oeuvre par la loi sur le commerce électronique (p. ex. la sécurisation des paiements et l'identification des cocontractants). Les réglementations relatives au commerce électronique et à la protection des données personnelles sont les pans d'une même toiture sous laquelle les opérateurs économiques pourront agir en toute sécurité juridique.

Le projet de loi nécessite cependant un certain nombre de corrections et de modifications qui seront évoquées dans le cadre du commentaire des articles.

1.3. Analyse critique de certains points fondamentaux du projet de loi

La Chambre des Métiers, sans vouloir sous-estimer la difficulté de la tâche de rédaction d'un projet de loi dans un domaine à haute technicité, déplore que le texte soit en partie difficilement compréhensible pour un non-spécialiste, et ce notamment en raison du fait de la technique de renvoi utilisée dans beaucoup d'articles.

Dans la mesure où il s'agit d'un texte que les entreprises, non-spécialistes en la matière, sont amenées à appliquer au quotidien, un texte avec une structuration plus rationnelle et avec une plus grande clarté aurait été de mise.

La meilleure garantie pour une bonne application d'un texte législatif ou réglementaire par les personnes concernées réside en effet dans la clarté et la simplicité de ses dispositions.

Il est également regrettable que les nombreux règlements d'exécution auxquels il est fait référence, ne soient pas disponibles au moment de l'analyse du projet de loi. Indépendamment du fait que les instances consultées et les députés ne sont pas en mesure d'apprécier la nouvelle réglementation dans toute sa forme et teneur, le projet de loi voté sans l'adoption parallèle des règlements d'exécution risque de rester lettre morte.

On peut par ailleurs s'interroger sur la pratique des règlements d'exécution dits „facultatifs“ prévus par le projet de loi. De deux choses l'une, ou bien un règlement d'exécution est nécessaire et par conséquent doit-il être obligatoirement prévu et être pris, ou bien il n'est pas nécessaire et il peut en être fait abstraction.

Force est par ailleurs de constater que le champ d'application du projet de loi est plus large que celui de la Directive en englobant par exemple les personnes morales, les personnes publiques et des domaines comme la défense, la sécurité publique, le droit pénal et la santé.

A cela s'ajoutent des dispositions spécifiques dans des domaines comme le traitement des données génétiques ou la surveillance sur le lieu de travail. La Chambre des Métiers, tout en étant consciente de

l'importance pour le Luxembourg d'avoir un cadre légal complet, se demande cependant s'il est opportun de tout vouloir régler dans un seul et même projet de loi.

Certaines de ces matières auraient plus logiquement leur place dans le cadre des législations spécifiques y relatives. Tel est notamment le cas pour la surveillance des salariés sur le lieu de travail et la liberté d'expression.

La Chambre des Métiers constate que le projet de loi s'applique indistinctement au secteur privé et au secteur public. Il est certainement logique d'aborder la protection des personnes à l'égard du traitement des données à caractère personnel dans son ensemble.

Mais la Chambre des Métiers, sans vouloir entrer dans cette problématique qui ne concerne pas directement ses ressortissants, se demande cependant s'il ne faudrait pas différencier certaines dispositions pour tenir compte des spécificités entre secteurs public et privé.

Il paraît par exemple difficile d'appliquer les règles de protection entourant les personnes soumises à une surveillance sur le lieu de travail, plus particulièrement celles impliquant le comité mixte d'entreprise ou une délégation de personnel, au service public, dans la mesure où ce dernier ne connaît pas ces institutions.

Le projet de loi prévoit qu'une Commission Nationale pour la Protection des Données remplace l'actuelle Commission consultative auprès du Ministre compétent. Une bonne application de la loi passe par l'institution d'une commission dotée des moyens nécessaires pour l'exercice de ses missions.

La Chambre des Métiers doute que la nouvelle Commission telle que prévue dans le projet de loi puisse faire efficacement son travail. Il est renvoyé à ce sujet aux observations du commentaire des articles.

1.4. Interconnexion des données „publiques" par l'autorisation d'utilisation d'une clé d'échange informatisée

La Chambre des Métiers a lu avec intérêt l'affirmation contenue dans l'exposé des motifs d'après laquelle une amélioration majeure et nécessaire au fonctionnement des administrations publiques va être apportée dans la mesure où celles-ci peuvent dorénavant, sous certaines conditions, interconnecter leurs différents fichiers. Il s'agit d'un changement important par rapport à la loi de 1979 qui avait exclu cette possibilité.

Le projet de loi soumet l'interconnexion de données à une autorisation préalable de la Commission nationale pour la protection des données.

La Chambre des Métiers est d'avis que l'interconnexion entre données „publiques" ne peut se faire raisonnablement que par l'utilisation d'une clé d'échange.

Or, le projet de loi, tout en prévoyant la possibilité d'interconnexion, n'y intègre pas le principe d'utilisation d'une clé d'échange informatisée, comme par exemple l'utilisation du numéro matricule.

Une interconnexion fiable et efficace, dont le numéro matricule national est un instrument de premier choix, est cependant indispensable pour permettre aux acteurs publics de profiter des opportunités de simplification offertes par la société de l'information. Or la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales laisse à des règlements grand-ducaux le soin de déterminer les actes, documents et fichiers qui pourront utiliser le numéro d'identité national à condition que celui-ci soit réservé à l'usage administratif interne ou aux relations avec le titulaire du numéro.

Le règlement grand-ducal du 7 juin 1979 déterminant les actes, documents et fichiers autorisés à utiliser le numéro d'identité, tel qu'il a été modifié par la suite, énumère les banques de données autorisées à utiliser le matricule en question. Comme le projet de loi est muet sur l'utilisation de la matricule nationale, la Chambre des Métiers propose d'intégrer l'utilisation du numéro matricule ou d'une clé d'échange informatisée à définir, dans l'autorisation du traitement (d'interconnexion) par la Commission Nationale pour la Protection des Données, et d'éviter ainsi que l'autorisation d'utilisation du numéro matricule reste juridiquement isolée (dans un scénario imaginable où le traitement d'échange aurait été autorisé).

La Chambre des Métiers invite les responsables politiques à réformer les règles d'utilisation du matricule dans le cadre des traitements informatiques.

*

2. COMMENTAIRE DES ARTICLES

Ad article 1 – Objet

Il résulte de cet article que la Directive s'applique non seulement aux personnes physiques, mais également aux personnes morales. L'extension aux personnes morales de la protection des données nominatives n'est pas prévue par la Directive.

Tout en étant consciente de l'importance d'une protection des personnes morales, la Chambre des Métiers est d'avis que la question de prévoir pour elles un régime analogue aux personnes physiques mériterait une réflexion approfondie au lieu d'être réglée à l'improviste dans le cadre de la transposition d'une Directive consacrée exclusivement aux personnes physiques.

La Chambre des Métiers est par ailleurs d'avis que cet article a plus le caractère d'une déclaration d'intention que d'une disposition normative.

Ad article 2 – Définitions

La Chambre des Métiers approuve l'utilisation par les auteurs du projet de loi de la technique des définitions légales qui sont de nature à préciser les concepts utilisés en vue d'une meilleure compréhension du texte. Cependant, elle se doit de faire quelques observations rédactionnelles.

Concernant le point (k), la Chambre des Métiers estime cependant qu'il y a lieu de préciser davantage ce qui est visé par „mission d'enquête particulière".

En outre, elle aimerait rendre attentif sur une erreur matérielle au niveau de l'énumération alphabétique dans la mesure où la page se termine avec le point (m) tandis que la page 3 commence avec (o).

Il ressort de la définition donnée du terme „organisme de sécurité sociale", que les compagnies d'assurances privées sont a priori aussi visées. Ceci paraît difficilement concevable. Ainsi, il ya lieu, le cas échéant, d'apporter les clarifications terminologiques nécessaires.

Le terme „pays tiers" n'a aux yeux de la Chambre des Métiers pas lieu d'être défini alors qu'il s'agit d'un terme consacré.

Ad article 3 – Champ d'application

Les auteurs du projet de loi ont opté pour un champ d'application très large incluant la défense, la sécurité publique, la sécurité de l'Etat et ses activités dans le domaine du droit pénal etc. Ils justifient cette approche par la nécessité de mettre en place un cadre juridique complet.

Compte tenu du caractère spécifique de ces matières qui ont trait à la puissance publique, la Chambre des Métiers est d'avis que le problème de la protection des données à caractère personnel devrait être réglé dans le cadre des législations respectives.

La Chambre des Métiers est par ailleurs d'avis que le terme „bien-être économique" recopié de la Directive sans autre explication, mériterait davantage de précision.

Ad article 4 – Qualités des données

Cet article pose le principe du respect des finalités des traitements, qu'on peut considérer comme principe de base de la protection des données. Les finalités doivent être explicites et légitimes et doivent être déterminées lors de la collecte des données.

Les finalités ultérieures à la collecte ne peuvent pas être incompatibles avec les finalités telles que spécifiées à l'origine. Ce principe novateur par rapport à la loi de 1979 présente certainement l'avantage qu'il ne peut pas être dépassé par la technologie car il s'exerce sur la personne qui utilise les données collectées.

Il ne faut cependant pas perdre de vue que le contrôle du respect du principe de finalité relève de l'appréciation des personnes en contact avec le traitement de données, appréciation qui peut diverger d'une personne à l'autre. Pour cette raison, il n'est pas indiqué de prévoir „obligatoirement" les sanctions pénales spécifiées dans l'article.

S'agissant d'une question d'appréciation avec tous les aléas que cela comporte, une sanction pénale facultative par l'introduction du terme „peut" serait plus appropriée.

L'article prévoit en outre qu'une autorisation doit être sollicitée au cas où les données traitées à des finalités déterminées seront ultérieurement traitées à des fins historiques, statistiques ou scientifiques.

Ne serait-il pas plus simple de garantir la protection des personnes en ayant tout simplement recours au mécanisme d'autorisation légale ou réglementaire?

Ad article 5 – Légitimité du traitement

Contrairement à la loi de 1979, le projet de loi énumère de manière explicite et limitative les cas dans lesquels les données à caractère personnel peuvent faire l'objet d'un traitement. Cela revient à dire qu'un traitement qui ne rentre pas dans un des six cas énumérés ne sera jamais autorisé.

Si la Chambre des Métiers peut souscrire à cette approche, qui a certainement le mérite d'être claire et précise, elle s'interroge cependant sur l'utilisation du terme „intérêt vital" employé sous e).

En effet, ce terme employé dans la Directive est un anglicisme qui résulte de la traduction littérale des mots „vital interest".

Or, le terme anglais paraît ambigu dans la mesure où, au sens strict, il est synonyme de question de vie ou de mort, il peut aussi désigner de façon plus large, un intérêt essentiel, capital, de première importance qui ne se rattache pas nécessairement à la survie de la personne concernée.

La Chambre des Métiers propose de retenir le terme de „sauvegarde de la vie de la personne concernée", terminologie recommandée par le professeur Guy BRAIBANT dans son rapport sur la transposition en droit français de la Directive.

A propos de la notion d'intérêt légitime figurant au point (d) de ce même article, la Chambre des Métiers souligne qu'il faut éviter d'interpréter cette notion de manière trop restrictive. Comme mentionné sous le point 1 ci-dessus, le traitement de données est devenu une composante vitale et essentielle de l'économie d'aujourd'hui.

Ad article 6 – Traitement de catégories particulières de données

L'article prévoit dans son paragraphe 1er les cas d'interdiction de traitement de certains types de données et dans son paragraphe 2 les cas où cette interdiction ne s'applique pas.

Le paragraphe 3 prévoit dans le cadre d'une procédure judiciaire les possibilités de traitement des données génétiques.

Tel est notamment le cas pour la répression d'une infraction ou pour la prévention „d'un danger concret", notion qui n'existe pas en droit pénal. Ne serait-il dans ces circonstances pas indiqué d'utiliser l'expression „prévention d'une infraction"?

Ad article 7 – Traitement de catégories particulières de données par les services de la santé

La Chambre des Métiers constate que le responsable du traitement est soumis au secret professionnel et les sous-traitants à la confidentialité.

Même s'il s'agit de notions à connotations différentes, les sanctions prévues en cas de violation du secret professionnel respectivement de la confidentialité sont les mêmes, à savoir une peine de prison de 8 jours à 6 mois et une peine d'amende. Ne serait-il pas indiqué de soumettre toute personne concernée par le traitement, la collecte ou la transmission de données au secret professionnel?

La Chambre des Métiers s'interroge par ailleurs sur la technique législative employée dans le présent article et consistant à prévoir la prise d'un règlement grand-ducal visant aussi les matières énoncées à l'article 6, technique qui ne contribue certainement pas à une bonne lisibilité du texte.

Ad article 8 – Traitement de données judiciaires

Les paragraphes 2 et 3 concernent le relevé des condamnations pénales (casier) qui doit être maintenu par l'autorité publique compétente en la matière ainsi que les jugements civils et administratifs.

La Chambre des Métiers propose d'y intégrer également la liste des protêts et le relevé des ordonnances de référé.

Il y a le cas échéant lieu de préciser quels services sont visés par le terme „autorité publique" compétente.

Ad article 10 – Traitement à des fins de surveillance

L'article définit les cas où la loi autorise le traitement à des fins de surveillance et définit les conditions dans lesquelles il peut être mis en oeuvre.

La Chambre des Métiers est d'accord pour dire qu'une telle surveillance doit se faire dans des cas limitativement prévus pour éviter le phénomène „big brother". Parmi les cas énumérés par le texte dans lequel la surveillance est nécessaire figure celui où la personne concernée a donné son consentement exprès. Toute surveillance est par ailleurs subordonnée à l'information des personnes concernées à l'aide de moyens appropriés.

Faut-il comprendre par là qu'en dépit d'une information au sens de la loi, la surveillance est interdite, si la personne concernée s'y oppose? Dans l'affirmative, quelle situation les auteurs du projet envisagent-ils?

Ad article 11 – Traitement à des fins de surveillance sur le lieu de travail

Cet article permet à l'employeur de contrôler, sous certaines conditions, les salariés sur le lieu de travail. Ainsi, un traitement à des fins de surveillance est possible pour des raisons de sécurité et de santé des travailleurs, de protection des biens de l'entreprise, de contrôle du processus de production ou du contrôle temporaire de production ou des prestations du travailleur en vue de mesurer son activité afin de déterminer sa rémunération.

La Chambre des Métiers, tout en accueillant favorablement l'introduction de ce droit en faveur de l'employeur, est cependant d'avis que la réglementation est loin de revêtir le caractère de précision et de clarté nécessaire.

Il serait utile de définir la notion de travailleur, qui doit se comprendre comme englobant les salariés au sens de l'article 1er de la loi du 24 mai 1989, ainsi que les stagiaires, apprentis, élèves et étudiants.

A la lecture des cas d'ouverture du droit de surveillance, il n'est pas clair si le contrôle par l'employeur de l'utilisation à des fins privés du matériel mis à disposition des salariés est prévu. Ce problème, qui n'est certes pas nouveau, revêt cependant une acuité particulière avec l'usage d'Internet et de la messagerie électronique par les salariés sur le lieu de travail.

Comme la jurisprudence luxembourgeoise, contrairement à la jurisprudence étrangère, est très peu fournie par rapport aux nouveaux moyens de communication, il serait dans l'intérêt de l'employeur et des salariés d'avoir une réglementation claire et précise à ce sujet, conciliant dans la transparence le droit légitime de contrôle de l'employeur, d'une part, avec le droit au respect de la vie privée des salariés, d'autre part.

La question du contrôle du courrier électronique mériterait en tout cas d'être traitée plus en détail dans le cadre de la législation du droit du travail.

Concernant l'information du comité mixte d'entreprise visé au paragraphe 1er, la Chambre des Métiers suggère de revoir la formulation („le cas échéant") qui laisse penser qu'un tel comité puisse être institué par les entreprises selon leur bon vouloir, ce qui n'est évidemment pas le cas, l'institution d'un tel comité étant prévue par la loi.

Ad article 12 – Obligation de notification à la Commission

Cet article pose le principe de la notification des traitements. Dans cette optique, la Commission contrôle a posteriori et non plus a priori, comme cela est prévu par la loi actuelle. Il prévoit même une dispense de notification en cas de traitement ayant pour seul objet la tenue d'un registre qui en vertu d'une disposition légale est destiné à l'information du public.

Il en va de même, au cas où un chargé de protection tenu d'assurer de manière indépendante l'application des dispositions légales en la matière, est nommé par le responsable du traitement. Concernant ce chargé, il est renvoyé aux observations sub article 40.

Ad article 13 – Contenu et forme de la notification

L'article 13 énumère les informations qu'une notification doit contenir. Il s'agit de la liste proposée dans la Directive, qui constitue un minimum, et à laquelle les auteurs du projet de loi proposent d'ajouter une information sur la durée de conservation des données.

La Chambre des Métiers n'est pas sûre de la valeur ajoutée d'une telle donnée; d'autant plus qu'il sera en pratique souvent difficile, voire impossible de donner des renseignements fiables à ce sujet.

Le paragraphe 3 prévoit que la notification se fait auprès de la Commission moyennant support papier ou informatique, c'est-à-dire sur disquette. La Chambre des Métiers propose de prévoir également la possibilité d'effectuer cette notification par voie électronique.

Ad article 14 – Autorisation préalable de la Commission

La règle d'autorisation préalable reste applicable à chaque fois que le traitement présente un risque intrinsèque d'atteinte au respect de la vie privée de la personne concernée, au regard de la nature des données traitées et de la finalité du traitement. Ainsi, une autorisation préalable sera nécessaire pour les traitements concernant les données génétiques, le crédit et la solvabilité de la personne concernée ou encore en cas d'interconnexion de données à caractère personnel.

L'article précise encore que les traitements prévus à l'article 7 sont „le cas échéant" soumis à l'autorisation préalable. Au lieu de cette terminologie imprécise, il est proposé de spécifier qu'il s'agit des traitements au sens de l'article 7 paragraphe 1er.

En outre, il est à noter que l'article ne contient pas, comme c'est le cas dans la loi de 1979, de délai endéans lequel une décision de la Commission doit intervenir. Un tel délai ne serait cependant pas dénué de fondement.

Dans ce contexte, la Chambre des Métiers plaide pour le renversement de la présomption selon laquelle le silence de l'administration pendant un certain délai vaut une décision de refus, mécanisme d'ailleurs préconisé par le Ministère des Classes Moyennes dans le cadre de l'actualisation du plan d'action en faveur des PME.

Ad article 16 – Interconnexion de données à caractère personnel

L'article 16 soumet tout projet d'interconnexion entre deux ou plusieurs traitements, que leurs responsables relèvent du secteur public ou privé, à l'autorisation préalable de la Commission. Elle examinera notamment la licéité du traitement et les garanties concernant la compatibilité des finalités des traitements à interconnecter.

Concernant l'interconnexion effectuée par les administrations, la Chambre des Métiers renvoie à ses développements sur le numéro matricule national, voire une autre clé d'échange informatisée à définir, dans le cadre des observations générales du présent avis. Il en va de même en ce qui concerne les règlements d'exécution qui „peuvent être pris".

Ad article 22 – Sécurité des traitements

L'article indique que le responsable doit prendre les mesures techniques et d'organisation appropriées pour assurer la protection des données qu'il traite. Les auteurs se sont limités à recopier la Directive sans fournir la moindre précision sur la nature et le genre de dispositions techniques à prendre. S'agissant d'une question essentielle, ces précisions méritent d'être fournies dans le cadre de la loi ou d'un règlement d'exécution.

Il est par ailleurs prévu que les mesures techniques mises en oeuvre pour assurer la protection des données traitées doivent faire l'objet d'un examen annuel dont le résultat est communiqué à la Commission.

Cette exigence, qui ne figure pas à l'article 17 de la Directive copiée par les auteurs du projet de loi, suscite de nombreuses interrogations d'ordre pratique: qui peut faire cet examen, sous quel forme cet examen doit-il être fait, etc.?

La Chambre des Métiers considère qu'il s'agit d'une charge administrative sans valeur ajoutée pour les entreprises, de sorte qu'il y a lieu de faire abstraction de cette disposition.

Le paragraphe 3 précise en reprenant intégralement le texte de la Directive, que les relations entre le responsable de traitement et un sous-traitant doivent être régies par un contrat ou un acte juridique …

Au paragraphe 4, il est précisé qu'aux fins de la conservation des preuves, les éléments du contrat doivent être consignés par écrit.

Comme il s'agit nécessairement d'un engagement synallagmatique, il est indiqué de faire abstraction du terme „acte juridique" et d'utiliser le terme „contrat". Il serait également indiqué de préciser que le caractère écrit du contrat est prévu à titre de preuve et de validité de la convention.

Ad article 24 – Secret professionnel

L'article prévoit que les personnes en relation avec le traitement de données et soumises au secret professionnel ne peuvent opposer ce secret à la Commission.

Il serait utile de préciser de manière générale pour toutes les personnes visées qu'au cas où elles sont tenues de révéler un renseignement soumis au secret professionnel, elles ne peuvent encourir de ce fait une sanction pénale ou civile.

Ad article 25 – Sanctions relatives à la confidentialité et à la sécurité des traitements

Le terme de confidentialité est employé tant dans l'article 21, que dans le présent article et dans l'article 25. L'article 24 en revanche parle du secret professionnel. Le titre du chapitre „confidentialité et sécurité des traitements", ne reflétant pas l'ensemble des dispositions, il conviendrait d'y inclure également la notion de secret professionnel.

Il est à noter que les auteurs du projet de loi, tout en opérant une distinction entre les personnes soumises au secret professionnel et celles tenues à la confidentialité, sanctionnent les violations respectives à ces principes par la même peine. Dans ce contexte, la Chambre des Métiers se demande s'il n'y a pas lieu de soumettre, à l'instar de la loi de 1979, l'ensemble des personnes intervenant dans l'exercice de leurs fonctions dans la collecte, le traitement, ou la transmission de données au secret professionnel.

Ad article 27 – Exceptions au droit à l'information de la personne concernée

Le présent article prévoit les cas où il peut être dérogé au droit à l'information au sens de l'article 26.

S'il est logique d'utiliser le terme „sauvegarder" en relation avec la sûreté de l'Etat, la défense, la sécurité publique, il ne l'est pas forcément par rapport au point (d).

Le paragraphe 3, reprenant textuellement l'article 10 de la Directive, prévoit une dérogation à l'article 26 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 (…)*".

Il s'agit de notions très vagues, qui ne sont pas autrement commentées dans l'exposé des motifs, de sorte qu'il faudra apprécier au cas par cas. Comme l'interprétation qui pourra en être faite risque de varier, la Chambre des Métiers se demande si l'application de sanctions pénales importantes est justifiée et s'il n'était pas plus logique de prévoir simplement des sanctions de nature administrative.

D'une manière générale, la Chambre des Métiers est d'avis qu'il serait plus judicieux d'adopter une approche plus sélective concernant les sanctions pénales. Ainsi, on pourrait réserver l'application des sanctions pénales pour les dispositions de la loi où la violation serait particulièrement grave et préjudiciable et prévoir des amendes d'ordre pour les autres cas de violation.

A noter que la Directive parle de „sanctions appropriées", ce qui ne veut pas forcément dire qu'il doit s'agir de sanctions pénales, de surcroît cumulées dans certains articles avec des sanctions administratives. Cette observation paraît s'imposer face au facteur d'appréciation inhérent à l'application de certaines dispositions de la loi.

Ad article 30 – Droit d'opposition de la personne concernée

Les données informatiques constituant une matière primordiale pour les entreprises, la Chambre des Métiers estime que l'article 21 c) relatif à la communication des données personnelles à des tiers à des fins de prospection ne doit pas être interprétée de manière trop restrictive. En effet, cet article risque d'alourdir considérablement le processus administratif lié à l'exploitation à des fins commerciales de banques de données.

A ce propos, la Chambre des Métiers est d'avis que le consentement respectif donné par la personne concernée lors de la collecte des données devrait suffir pour pouvoir communiquer les données à caractère personnel à des tiers à des fins de prospection. En effet, le coût de la notification à la personne concernée risque d'augmenter d'une manière excessive l'investissement temporel et financier mis en oeuvre.

Concernant l'amende pénale, la Chambre des Métiers invite les auteurs du projet de loi de libeller le montant des amendes en euros.

Ad article 32 – Généralités

L'article énonce qu'à côté des actions en responsabilité prévues par le droit commun, un recours devant la Chambre du Conseil est possible.

Il reste cependant muet sur la nature du recours visé et sur les actes contre lesquels un recours serait possible.

Le texte, sans le dire expressément, vise plus particulièrement les actions en responsabilité civile sur base de l'article 1382 et de l'article 1384 alinéa 1er du Code Civil.

L'article 23 de la Directive désigne expressément, et ce contrairement à notre droit national, la personne qui en cas de responsabilité doit réparer le dommage subi. La Chambre des Métiers se demande dès lors s'il n'y a pas lieu de modifier l'article 1384 al. 1er du Code Civil sur ce point.

Ad article 33 – Recours devant la Chambre du Conseil

En cas de traitement mis en oeuvre en violation des formalités prévues par la présente loi et relatives à la publicité, à la procédure de notification ou d'autorisation préalable, la Chambre du Conseil dûment saisie, peut en cas d'indices suffisants, ordonner la suspension provisoire de l'activité, ou le cas échéant, la fermeture provisoire de l'établissement du responsable du traitement, et ce aussi longtemps que les formalités en violation desquelles le traitement a été mis en oeuvre ne sont pas réalisées.

Si la Chambre des Métiers peut souscrire au principe de sanction tel que proposé, analogue à celui existant en matière du droit d'établissement, elle est cependant d'avis que ce type de sanctions n'est pas concevable à l'encontre des administrations. Ne faudrait-il pas exclure le secteur public du régime de sanction?

Elle ne peut pas suivre les auteurs du projet de loi dans leur argumentaire développé dans l'exposé des motifs. La procédure proposée permet assurément de réagir rapidement par rapport à des abus manifestes.

Voir dans cette procédure, comme le suggère l'exposé des motifs, un moyen de favoriser la prise de conscience des gens, relève d'une mauvaise plaisanterie si l'on sait qu'en raison de la carence de l'Etat, la protection des données sous l'empire de la loi de 1979 n'était que partiellement, sinon aucunement appliquée ces dernières années.

Ad article 34 – Missions et pouvoirs de la Commission Nationale pour la Protection des Données

Une autorité de contrôle dénommée „Commission Nationale pour la protection des données" est chargée de vérifier la conformité des traitements de données par rapport aux dispositions de la présente loi.

L'article sous rubrique, tout en précisant au paragraphe (7) que la Commission peut ester en justice, reste cependant complètement muet sur son statut, qui ne se trouve précisé qu'à l'article 36, intitulé „Composition de la Commission Nationale pour la Protection des Données".

La Chambre des Métiers trouverait plus cohérent et logique de préciser d'abord de quel type d'organisme de contrôle il s'agit et de préciser ensuite ses missions, ses pouvoirs, son fonctionnement et son contrôle.

Les auteurs du projet ont opté pour le statut de l'établissement public et ce pour des raisons d'indépendance exigées par la Directive.

Force est de constater que la Commission se voit investie de pouvoirs très importants et multiples: elle est instance de contrôle, d'investigation, de recours, de coopération et de sanction.

Ce cumul impressionnant de fonctions n'est pas à l'abri de critiques par rapport aux principes fondamentaux de la séparation des pouvoirs et de la protection des droits des personnes.

Le texte ne précise par ailleurs pas quel est le pouvoir du personnel de la Commission, amené dans le cadre de leur pouvoir d'investigation à se rendre dans les entreprises.

Peuvent-ils venir librement sans avertissement préalable? Le droit d'accès s'étend-il à toutes les dépendances de l'entreprise? Peuvent-ils interroger le personnel de l'entreprise? En cas de refus de l'entreprise, est-ce que la Commission peut faire appel à la police grand-ducale? Est-ce que la Commission, qui d'après le paragraphe (7) peut dénoncer les infractions aux autorités judiciaires, est censée dresser, à l'instar de l'Inspection du Travail par exemple, des procès-verbaux transmis au Parquet?

Le texte autorise toute personne, ou *une association la représentant*, à saisir la Commission pour une question relative au respect de ses droits. A part la question de l'intérêt que peut avoir une personne de passer par une association, le texte semble vouloir dire que toute association, quel que soit son objet, a le droit de saisir la Commission. Cette disposition mériterait un certain nombre de précisions.

Le projet de loi précise que la Commission peut se faire assister dans l'exercice de ses nombreuses missions par des agents nommés et placés sous son autorité. Il ne contient cependant pas beaucoup de précisions sur la structure administrative de la Commission qui sera mise en place. Faut-il comprendre que ces agents seront regroupés dans une sorte de secrétariat administratif, chargé d'instruire les dossiers, soumis ensuite pour décision aux membres de la Commissions nommés par le Grand-Duc?

Compte tenu de l'importance d'un bon fonctionnement de cette institution à la suite de la piètre prestation de l'actuelle Commission consultative, une vision plus précise des choses serait souhaitable.

Ad article 35 – Sanctions administratives

Sans préjudice des poursuites pénales éventuelles et des sanctions pénales susceptibles d'en résulter, le paragraphe 1er prévoit que la Commission peut prononcer une amende d'ordre de maximum 500.000.– LUF à l'encontre d'une personne physique et de maximum 10.000.000.– LUF à l'encontre d'une personne morale, amende susceptible d'être doublée en cas de récidive.

Indépendamment de la nature des amendes d'ordre, qui, au regard de la Convention Européenne des droits de l'Homme, sont à qualifier de sanctions pénales, et de la question de la compatibilité de ce type d'amendes avec les règles sur les droits de l'Homme, l'articulation du système des sanctions administratives avec les décisions prises par la Chambre du Conseil de l'article 33 devra être précisée.

Concernant les sanctions administratives énumérées, il est à noter qu'il ne résulte pas clairement du paragraphe 1er quels types de violations sont visés.

Or, le principe de la légalité des incriminations exige que la loi indique clairement, le cas échéant par référence aux dispositions visées, quelle(s) violation(s) est(sont) sanctionnée(s).

Qu'en est-il par ailleurs de l'application de ces amendes aux pouvoirs publics?

La Chambre des Métiers conteste en tout cas le bien-fondé d'une amende d'ordre se chiffrant à 10.000.000.– pour une personne morale, montant disproportionné par rapport au but de la loi et susceptible de mettre en graves difficultés financières, sinon en faillite, un certain nombre d'entreprises.

Le paragraphe 2 provoit qu'en sus de l'amende d'ordre plusieurs sanctions disciplinaires peuvent être prononcées.

Il y a lieu d'enlever dans la première phrase du paragraphe 2 le mot „soit" qui ne donne aucun sens.

De plus, le terme même de „sanction disciplinaire" semble aux yeux de la Chambre des Métiers parfaitement inadéquat, alors qu'il vise de façon générale des sanctions prises à l'encontre d'un fonctionnaire coupable d'agissements contraires à son statut ou aux lois et règlements et non des sanctions suceptibles d'être prises à l'égard d'une personne du secteur privé.

Parmi les sanctions figure celle qui consiste à avertir ou à admonester le responsable du traitement.

Il paraît difficilement concevable que des sanctions du type de verrouillage ou destruction de données puissent être prises par la Commission sans autorisation judiciaire préalable.

L'insertion de la décision d'interdiction dans la presse n'étant pas une sanction en soi, mais une mesure accompagnant une sanction, la Chambre des Métiers est d'avis qu'elle ne devrait pas faire l'objet d'un point spécifique dans l'énumération des sanctions disciplinaires.

Il ressort encore du texte que les sanctions précitées seront prises dans le respect du contradictoire et des droits de la défense, l'application de ces principes pouvant être précisée dans un règlement d'exécution.

Il s'agit d'une disposition curieuse, dans la mesure où il est évident qu'il ne peut en être autrement.

La Chambre des Métiers constate également qu'il n'est nullement précisé quelles sont les possibilités de recours contre une décision de la Commission. Il y a par conséquent lieu de compléter le présent article en précisant la nature du recours – il ne peut s'agir que d'un recours devant le tribunal administratif – et de préciser s'il s'agit d'un recours en réformation ou en annulation.

On peut enfin s'interroger sur la conformité du système de sanction de l'article 35 avec l'article 28 de la Directive qui prévoit à titre de sanction uniquement l'avertissement et l'admonestation.

D'une manière générale, la Chambre des Métiers est surprise par l'approche adoptée par les auteurs du projet de loi qui consiste à suspendre au-dessus de la tête des entreprises une épée de Damoclès sous forme de toute une série de sanctions administratives et pénales.

Il n'est pas sûr qu'une telle approche, purement répressive, soit le meilleur moyen pour assurer une bonne application d'un texte de loi.

Ad article 36 – Composition de la Commission Nationale pour la Protection des Données

L'article 36 précise que la Commission est composée de trois membres effectifs et de trois membres suppléants dont un président et un vice-président nommés par le Grand-Duc.

Compte tenu de l'importance et du nombre de ses missions, la Commission devrait aux yeux de la Chambre des Métiers comporter plus de membres.

Elle est également d'avis que la représentation des différents milieux socioprofessionnels concernés par cette loi, allant de représentants du secteur public aux entreprises, aux consommateurs, … doit être assurée.

Ad article 37 – Fonctionnement de la Commission Nationale pour la Protection des Données

La Chambre des Métiers s'interroge sur certains aspects du fonctionnement de la Commission.

Il semble y avoir un défaut de cohérence entre l'article 36 paragraphe 2 et l'article 37 paragraphe (1) c. Etant donné que le président et le vice-président sont nommés par la Commission, il n'y a plus lieu de fixer les modalités de nomination dont fait état l'article 37 paragraphe (1) c.

La Chambre des Métiers a par ailleurs du mal à comprendre pourquoi il faudrait distinguer dans une Commission composée de trois membres, entre „majorité absolue" et „majorité d'au moins deux voix".

Ad article 38 – Statut des membres et agents de la Commission Nationale pour la Protection des Données

La Chambre des Métiers est d'avis que le texte ne fournit pas assez de précisions par rapport aux différentes personnes susceptibles d'être placées sous l'autorité de la Commission. Le texte utilise tantôt le terme d'agents, d'ouvriers, d'employés. Il ne précise par ailleurs pas le statut de ceux effectuant des contrôles sur le terrain. Y'a-t-il parmi ces personnes, des personnes ayant le statut d'officier de police judiciaire?

Ad article 40 – Le chargé de la protection des données

Le texte introduit un chargé de la protection des données, pratique bien connue en droit allemand.

On peut lire dans l'exposé des motifs que l'intérêt pratique d'un tel chargé, dont les missions se substituent en partie à celles de la Commission, est de sensibiliser les salariés à la protection des données et de limiter l'ampleur bureaucratique de contrôle. La Chambre d'es Métiers constate qu'il n'y a pas d'analyse sur la plus-value d'une telle institution, génératrice de coûts pour les entreprises susceptibles d'y recourir.

Il n'est de surcroît nullement établi qu'une telle profession soit nécessaire pour la bonne application de la loi au cas où la Commission fonctionne de façon efficace et compétente. Sauf erreur ou omission, un pays comme la France connaît avec la CNIL un organe de contrôle qui fonctionne de façon efficace sans un tel chargé de protection des données.

Aux yeux de la Chambre des Métiers, l'introduction d'un tel chargé pourrait éventuellement être discutée au moment où l'on peut tirer les premiers enseignements de l'application de la nouvelle loi et du rôle joué par la Commission.

Indépendamment de ce qui précède, la Chambre des Métiers estime que le montant de 15 millions de francs, exigé pour des raisons d'indépendance à titre d'assise financière, est excessif et discriminatoire.

La Chambre des Métiers, après consultation de ses ressortissants, et sous réserve des observations précitées, peut approuver le projet de loi sous avis.

Luxembourg, le 22 novembre 2001.

Pour la Chambre des Métiers,

Le Directeur,
Paul ENSCH

Le Président,
Paul RECKINGER

4735/02A

N° 4735[2A]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

A la demande de Monsieur le Ministre délégué aux Communications en date du 14.1.2002, le document parlementaire No 4735[2] concernant le projet de loi repris sous rubrique est retiré et est à considérer comme nul et non avenu.

Service Central des Imprimés de l'Etat

4735/06

N° 4735[6]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

AVIS DU CONSEIL D'ETAT

(29.1.2002)

Par dépêche du 19 décembre 2000, le Premier Ministre, Ministre d'Etat, soumit à l'avis du Conseil d'Etat le projet de loi sous rubrique, élaboré par le ministre délégué aux Communications.

Au texte du projet étaient joints l'exposé des motifs, le commentaire des articles ainsi que la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Le 28 juin 2001, le Conseil d'Etat fut saisi de l'avis de la Chambre des fonctionnaires et employés publics. Les avis respectifs de la Chambre de travail et de la Chambre des employés privés lui parvinrent par dépêche du 26 novembre 2001. L'avis de la Chambre des métiers lui fut transmis le 29 novembre 2001. A sa demande du 17 septembre 2001, le Conseil d'Etat s'est encore vu communiquer le 3 octobre 2001 l'avis du Procureur général d'Etat du 5 juillet 2001.

Le projet de loi sous examen a pour objet de traduire en droit national les obligations imposées aux Etats membres de l'Union européenne par la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1].

Une première initiative de transposition – il est vrai annoncée dès le départ comme partielle – de la directive par le projet de loi No 4357 relative au respect du droit à la vie privée à l'égard du traitement des données à caractère personnel, déposé le 8 octobre 1997, a avorté. Comme ledit acte communautaire aurait cependant, en vertu de son article 32, dû être répercuté en droit national depuis le 24 octobre 1998, le Grand-Duché de Luxembourg se trouve actuellement dans le collimateur des instances européennes. C'est ainsi que la Commission a décidé le 29 juillet 1999 d'adresser un avis motivé au Luxembourg[2] pour non-communication des mesures nécessaires à la transposition de la directive 95/46/CE. Le 20 septembre 1999, elle se résolut à engager, sur la base de l'article 226 du traité CE, une action en justice contre notre pays[3].

Ce manquement ne nous amène pas seulement dans une situation inconfortable au niveau communautaire, mais risque par ailleurs d'engendrer des effets contraignants en droit interne. En effet, dans les Etats membres qui n'ont pas encore pris les mesures de transposition nécessaires, les particuliers peuvent invoquer certaines dispositions d'une directive devant le juge national qui est tenu d'interpréter le droit national, „dans toute la mesure possible, à la lumière du texte et de la finalité de la directive pour atteindre le résultat visé par celle-ci et se conformer ainsi à l'article 189, troisième alinéa, du traité"[4]. Et „lorsque … un Etat membre méconnaît l'obligation qui lui incombe en vertu de l'article 189, troisième alinéa, du traité, de prendre toutes les mesures nécessaires pour atteindre le résultat prescrit par une

1 publiée au J.O.C.E. No L 281 du 23.11.1995 et ci-après appelée „la directive"

2 ainsi qu'à la France, aux Pays-Bas, au Royaume-Uni, à l'Irlande, au Danemark, à l'Espagne et à l'Autriche

3 de même que contre la France, les Pays-Bas, l'Allemagne et l'Irlande

4 C.J.C.E. arrêt du 13.11.1990, aff. *Marleasing* C-106/89; Recueil 1990 p. I – 4135, considérant 8

directive, la pleine efficacité de cette norme de droit communautaire impose un droit à réparation dès lors que trois conditions sont réunies. La première de ces conditions est que le résultat prescrit par la directive comporte l'attribution de droits au profit de particuliers. La deuxième condition est que le contenu de ces droits puisse être identifié sur la base des dispositions de la directive. Enfin, la troisième condition est l'existence d'un lien de causalité entre la violation de l'obligation qui incombe à l'Etat et le dommage subi par les personnes lésées. Ces conditions sont suffisantes pour engendrer au profit des particuliers un droit à obtenir réparation, qui trouve directement son fondement dans le droit communautaire".[1]

*

CONSIDERATIONS GENERALES

L'exposé des motifs, méthodique et exhaustif, dispense le Conseil d'Etat de retracer l'historique du projet de loi sous avis. Les auteurs du projet ont réussi, avec une rare acribie, d'en expliquer les tenants et aboutissants[2]. Aussi le Conseil d'Etat se borne-t-il à cerner de plus près la problématique inhérente à la genèse de la directive et à placer le projet en question sous l'éclairage particulier du droit international, avant d'aborder quelques aspects particuliers de la réforme projetée.

La directive 95/46/CE

L'intérêt et la nécessité de protéger la vie privée, dans une société de l'information et de la communication placée sous l'emprise envahissante des progrès frénétiques de la technologie, ont été soulignés en ces termes dans le rapport soumis en 1994 par le groupe *Bangemann* au Conseil européen:

> „L'exigence de la protection de la vie privée augmentera à juste titre, à mesure qu'il deviendra possible, grâce aux nouvelles technologies, d'obtenir et de manipuler (même au-delà des frontières nationales) des informations détaillées sur les personnes, en provenance de différentes sources de données, sons et images. Sans la sécurité juridique qu'offrirait l'adoption d'une politique commune à l'échelle de l'Union, le manque de confiance du consommateur freinerait sûrement le développement rapide de la société de l'information.
>
> L'Europe joue, dans le monde, un rôle moteur en faveur de la protection des droits fondamentaux dans le domaine du traitement des données à caractère personnel. L'application des nouvelles technologies risque de toucher des aspects très sensibles ayant trait, par exemple, aux images des personnes, à leurs relations, à leurs déplacements et à leur comportement. Il est très possible qu'en réaction, la plupart des Etats membres adoptent des mesures de protection, telles que le contrôle transfrontalier des nouvelles technologies et des nouveaux services.
>
> Les disparités des niveaux de protection de ces réglementations nationales en matière de vie privée pourraient amener les autorités nationales à restreindre la libre circulation entre les Etats membres d'une large gamme de nouveaux services, afin de protéger les données à caractère personnel.
>
> Le groupe estime que, sans la sécurité juridique offerte par l'adoption d'une politique à l'échelle de l'Union, le manque de confiance des consommateurs freinerait sûrement l'instauration rapide de la société de l'information. Compte tenu de l'importance et du caractère particulièrement sensible de la question de la vie privée, les Etats membres doivent prendre rapidement une décision sur la proposition de directive de la Commission définissant des principes généraux en matière de protection des données."[3]

Les conclusions du rapport *Bangemann* furent entérinées par le Conseil européen des 24 et 25 juin 1994 à Corfou, qui invita „le Conseil et le Parlement à adopter, avant la fin de l'année, des mesures dans les domaines déjà couverts par des propositions existantes. Il invite également la Commission à

---

1 C.J.C.E. arrêt du 19.11.1991, aff. *Francovich* C-6/90 et C-9/90; Recueil 1991 p. I – 5357, considérants 39 à 41

2 Pour un résumé de l'historique et des dispositions principales, il est renvoyé à la Conférence de presse de M. le Ministre Biltgen du 13 décembre 2000

3 Bruxelles, le 26 mai 1994 / L'Europe et la société de l'information planétaire / Recommandations au Conseil européen / Chapitre III sous Respect de la vie privée

définir dès que possible un programme qui porte sur les autres mesures nécessaires au niveau communautaire".[1]

C'est dans ce contexte que se situe la directive 95/46/CE du 24 octobre 1995.

La directive trouve son fondement juridique dans l'article 100A (actuellement 95) du traité instituant la Communauté européenne qui renvoie expressément à son article 7A (actuellement 14) qui vise le marché intérieur comportant „un espace sans frontières intérieures dans lequel la libre circulation des marchandises, des personnes, des services et des capitaux est assurée selon les dispositions du (présent) traité". Cet espace sans frontières que constitue le marché intérieur doit cependant, au vœu de cette même directive, rester régi par les principes découlant de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ainsi que de la Convention, du 28 janvier 1981[2], du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.[3]

La directive s'évertue ainsi à mettre en balance les intérêts économiques prévalant à l'intérieur du marché commun et les libertés et droits fondamentaux des personnes à protéger dans le cadre de la libre circulation des données à caractère personnel. Il s'agit sans doute d'un exercice périlleux, d'autant plus que les enjeux commerciaux sont considérables. Il n'est pas sûr non plus qu'un arbitrage équitable entre ces objectifs, rarement convergents, puisse toujours être assuré. Ce tiraillement inhérent aux objectifs de la directive ne manquera pas de provoquer des conflits ardus que des commentateurs[4] ont préfiguré comme suit:

> „En réalité, le but véritable de la directive est d'éviter que la libre circulation de l'information entre Etats membres, liberté par essence économique, soit excessivement limitée – au surplus de manière différente au sein de chaque Etat – au nom de droits et libertés de la personne humaine. Dans la mesure où l'objectif premier de l'Union européenne est la création d'un marché sans frontières internes, assurant la libre circulation des marchandises, personnes, services et capitaux, la libre circulation des données apparaît comme une condition indispensable de la création effective de ce marché. Cette libre circulation exige qu'une protection des droits fondamentaux des personnes concernées par ces données soit assurée sinon de manière uniforme, du moins de façon équivalente dans les divers Etats membres, étant entendu qu'elle s'opère, selon les déclarations des considérants, à un niveau élevé.
>
> On peut prévoir qu'à l'avenir, les législations nationales de protection des données deviendront, plus que jamais, le terrain d'une confrontation incessante entre, d'une part les intérêts économiques et commerciaux de responsables de traitements qui n'auront de cesse de légitimer leurs traitements sur les grandes libertés économiques fondant l'Union européenne, et plus précisément sur l'„équilibre" consacré par les dispositions de la directive commentée, et d'autre part, les intérêts de la personne concernée par les données qui mettra en avant les droits et libertés fondamentales qui lui sont reconnus au sein de chaque Etat membre sur la base des conventions et autres instruments issus du Conseil de l'Europe. Les oppositions pourront d'ailleurs surgir lors d'applications non spécifiques à la libre circulation de l'information, mais par exemple à la liberté de concurrence ou d'établissement.
>
> C'est d'autant plus vrai que les protagonistes disposeront dans l'avenir de voies juridictionnelles différentes afin de tenter de résoudre les probables conflits. Les responsables des traitements préféreront certainement utiliser la voie des procédures introduites devant la Cour européenne de Luxembourg. Les personnes concernées opteront plutôt pour les procédures propres à la Convention européenne des droits de l'homme devant la Cour de Strasbourg. Même si l'on peut s'attendre à des rapprochements entre l'Union européenne et le Conseil de l'Europe, les différences de fondement de l'intervention des organes conjointement compétents risquent de déboucher sur des solutions difficilement conciliables."[5]

---

1 Conclusions de la présidence (pt 4)

2 approuvée par la loi du 19.11.1987 (Mém. A 1987, p. 2069)

3 Voir considérants 1, 2, 3, 10, 11 et 37 de la directive

4 Marie-Hélène Boulanger, Cécile de Terwangne, Thierry Léonard, Sophie Louveaux, Damien Moreau, Yves Poullet „La protection des données à caractère personnel en droit communautaire" J.T.D.E. livraisons de juin, septembre et octobre 1997

5 ibidem pts 4 et 5

Il est intéressant de souligner à ce propos que la Charte des droits fondamentaux de l'Union européenne, telle qu'elle a été signée et proclamée par les Présidents du Parlement européen, du Conseil et de la Commission lors du Conseil européen de Nice le 7 décembre 2000, met quant à elle l'accent sur la protection des intérêts de la personne en stipulant dans son article 8 que:

„*Protection des données à caractère personnel*

1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante."[1]

Le droit international

La directive 95/46/CE prend soin de faire remarquer par son considérant 11 que „les principes de la protection des droits et des libertés des personnes, notamment du droit à la vie privée, contenus dans la (présente) directive précisent et amplifient ceux qui sont contenus dans la convention, du 28 janvier 1981, du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel". Il est intéressant de signaler dans ce contexte que, lors de sa réunion à Strasbourg, le 15 juin 1999, le Comité des Ministres a adopté une série d'amendements à la Convention du 28 janvier 1981, afin de permettre l'adhésion des Communautés européennes.

Le Grand-Duché de Luxembourg en tant que partie liée par la convention précitée, au même titre d'ailleurs que les autres Etats membres de l'Union européenne[2], se doit évidemment d'effectuer l'œuvre de transposition de la directive dans le respect de ses obligations internationales. Le Conseil d'Etat aura encore l'occasion de le rappeler dans le cadre de son examen des articles.

Aussi faudra-t-il tenir compte de la Convention d'application de l'Accord de Schengen du 14 juin 1985[3] qui renvoie quant à elle et à la convention précitée du 28 janvier 1981 et au droit communautaire, en stipulant que:

„*Article 126*

1. En ce qui concerne le traitement automatisé de données à caractère personnel qui sont transmises en application de la présente Convention, chaque Partie Contractante prendra au plus tard au moment de l'entrée en vigueur de la présente Convention les dispositions nationales nécessaires aux fins de réaliser un niveau de protection des données à caractère personnel qui soit au moins égal à celui découlant des principes de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

…

Article 134

Les dispositions de la présente Convention ne sont applicables que dans la mesure où elles sont compatibles avec le droit communautaire."

Il ne doit pas surprendre que dans ce contexte de renvois croisés entre normes de droit communautaire et international, système rappelant étrangement la théorie des vases communicants, la détermination des dispositions applicables dans un cas concret relève parfois de la gageure. Dans un tel imbroglio, la sécurité juridique n'a rien à gagner, ce qui est d'autant plus regrettable qu'il y va des libertés et droits fondamentaux.

Quelques aspects particuliers de la réforme

A cet endroit, le Conseil d'Etat se propose de développer quelques aspects particuliers du projet de loi sous avis en insistant plus longuement sur le système des sanctions pénales et administratives.

---

1 J.O.C.E. No C 364 du 18.12.2000

2 Cette convention est actuellement en vigueur entre les Etats suivants: Allemagne, Autriche, Belgique, Danemark, Espagne, Finlande, France, Grèce, Irlande, Islande, Italie, Luxembourg, Norvège, Pays-Bas, Portugal, Royaume-Uni, Slovénie, Suède, Suisse. Elle a encore été signée par Chypre, la Hongrie, la Roumanie et la Turquie

3 approuvée par une loi du 23 juillet 1992 et publiée au Mém. A 1992, p. 1574

Le système institué par le projet de loi

La loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques subordonne la création et l'exploitation de toute banque de données ne relevant pas de l'Etat à une autorisation ministérielle préalable.[1] Pour les raisons plus amplement développées dans son exposé des motifs, le projet de loi sous examen se propose de remplacer le système existant par une procédure moins lourde et plus expéditive.

Il prévoit ainsi de soumettre le traitement de données à caractère personnel non plus à une procédure d'autorisation, mais à un système de notification préalable.[2] A noter que cette obligation de notification n'est même pas générale, des exemptions étant données dans un certain nombre d'hypothèses.[3] L'autorisation préalable n'aura plus qu'un caractère résiduel dans le contexte du traitement de données particulièrement sensibles.[4]

Le système en vue tel qu'esquissé ci-dessus constitue un allégement manifeste des règles en vigueur, largement restées lettre morte à cause de leur inapplicabilité dans le contexte du changement fondamental intervenu en matière informatique et électronique depuis 1979.

L'approche des auteurs constitue donc un pas dans la bonne direction. Reste à espérer que la Commission nationale pour la protection des données à instituer disposera des moyens matériels et personnels nécessaires pour remplir ses tâches qui sont importantes et complexes.

Le projet de loi, un projet-cadre

Au vœu de la directive 95/46/CE, „les Etats membres sont habilités à assurer la mise en œuvre de la protection des personnes, tant par une loi générale relative à la protection des personnes à l'égard du traitement des données à caractère personnel que par des lois sectorielles telles que celles par exemple aux instituts de statistiques".[5] Les auteurs du projet de loi sous revue ont opté pour une loi-cadre.[6] Il n'en demeure pas moins qu'ils se sont nécessairement vu amenés à reconnaître un lien certain avec différentes dispositions légales en vigueur, relatives notamment à la loi du 14 août 2000 relative au commerce électronique ou encore à celle du 28 août 1998 sur les établissements hospitaliers.

Force est de relever encore que différents articles du projet de loi en cause risquent d'interférer avec des projets en voie d'élaboration parallèle. Il s'agit plus particulièrement des articles 11 et 9 en rapport idéal avec les réformes envisagées en matière de travail et de presse. Surtout au regard de cette dernière, il se recommande de faire preuve d'une attention vigilante en veillant à une démarche dans l'ensemble cohérente. Le Conseil d'Etat y reviendra à l'occasion de l'examen des articles en cause.

Les sanctions prévues

La directive 95/46/CE prévoit dans son article 24 que „les Etats membres prennent les mesures appropriées pour assurer la pleine application des dispositions de la (présente) directive et déterminent notamment les sanctions à appliquer en cas de violation des dispositions prises en application de la (présente) directive".

Le projet de loi répertorie pas moins de vingt cas de comportements passibles de peines correctionnelles, la peine d'emprisonnement prévue variant entre 8 jours et un an et l'amende se situant dans une fourchette allant de 10.001 à 5.000.000 de francs.

Sans préjudice de ces peines pénales, le projet de loi sous revue investit par son article 35 la Commission nationale pour la protection des données du pouvoir d'émettre des sanctions administratives substantielles. Ces amendes d'ordre peuvent en effet atteindre 10.000.000 de francs lorsqu'il s'agit d'une personne morale et 500.000 francs lorsqu'il s'agit d'une personne physique, les montants étant doublés en cas de récidive.

---

1 Voir article 4 de cette loi

2 Article 1er, paragraphe 1er du projet

3 Article 12, paragraphe 2 du projet

4 Article 14

5 Considérant 23 de la directive 95/46/CE

6 Voir point II 3 de l'exposé des motifs, Article 14

Le Conseil d'Etat se demande si les auteurs du projet de loi sous examen ne pèchent pas par un excès de répression en cumulant ainsi sanctions pénales et sanctions administratives et en multipliant les faits répréhensibles.

Quant aux sanctions pénales

Le nombre de comportements sujets à des peines correctionnelles est impressionnant. Le tableau synoptique ci-après reproduit est fort éloquent à ce sujet.

Tableau synoptique des sanctions pénales prévues

Cas	*Article*	*Fait incriminé*	*Pénalité*
1	4, par. (3)	– violation par le responsable du traitement, de l'obligation de garantir le traitement loyal et licite des données	Emprisonnement de 8 jours à 6 mois et/ou amende de 10.001 à 3.000.000 LUF
2	5, par. (2)	– traitement illégitime de données	Idem
3	6, par. (5)	– traitement révélant, en dehors des cas prévus par la loi, l'origine raciale ou ethnique, les origines politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé et à la vie sexuelle d'une personne	Emprisonnement de 8 jours à 1 an et/ou amende de 10.001 à 5.000.000 LUF
4	7, par. (5)	– traitement illégal de données particulières par les services de la santé	Idem
5	8, par. (4)	– traitement illégal de données judiciaires	Idem
6	10, par. (5)	– violation des dispositions régissant le traitement (de données) à des fins de surveillance	Idem
7	11, par. (3)	– violation des dispositions concernant le traitement (de données) à des fins de surveillance sur le lieu de travail	Idem
8	12, par. (3)	– omission de notification d'un traitement à la Commission nationale	Amende de 10.001 à 1.000.000 LUF
9	12, par. (4)	– information sciemment incomplète ou inexacte de la Commission nationale	Emprisonnement de 8 jours à 6 mois et/ou amende de 10.001 à 3.000.000 LUF
10	13, par. (4)	– information incomplète de la Commission ou mise en œuvre du traitement avant notification des modifications affectant les informations originaires	Amende de 10.001 à 1.000.000 LUF
11	14, par. (3)	– traitement sans autorisation préalable	Emprisonnement de 8 jours à 1 an et/ou amende de 10.001 à 5.000.000 LUF
12	17, par. (3)	– mise en œuvre d'un traitement non institué par voie réglementaire	Idem
13	18, par. (5) 9, par. (4)	– transfert illégal de données vers un pays tiers	Idem
14	25	– violation des règles relatives à la confidentialité ou à la sécurité des traitements	Emprisonnement de 8 jours à 6 mois et/ou amende de 10.001 à 3.000.000 LUF
15	26, par. (4)	– violation du droit d'information de la personne concernée	Emprisonnement de 8 jours à 1 an et/ou amende de 10.001 à 5.000.000 LUF
16	28, par. (2) 28, par. (8)	– entrave de l'exercice du droit d'accès – faux usage du droit d'accès	Idem

Cas	*Article*	*Fait incriminé*	*Pénalité*
17	29, par. (5)	– mauvais usage par le responsable du traitement de son droit de limiter ou différer l'exercice du droit d'accès	Idem
18	30, par. (4)	– entrave du droit d'opposition de la personne concernée	Emprisonnement de 8 jours à 1 an et/ou amende de 10.001 à 3.000.000 LUF
19	33, par. (13)	– manquement à l'ordonnance d'une chambre du Conseil	Emprisonnement de 8 jours à 6 mois et/ou amende de 10.001 à 3.000.000 LUF
20	34, par. (10)	– obstruction à l'action de la Commission nationale	Emprisonnement de 8 jours à 1 an et/ou amende de 10.001 à 5.000.000 LUF

Le Conseil d'Etat croit déceler quelques inconséquences dans ce répertoire imposant.

L'échelle des sanctions prévues n'est pas toujours évidente. Le Conseil d'Etat aura l'occasion d'illustrer son propos lors de l'examen des articles. Qu'il soit simplement fait remarquer à ce stade et à titre d'exemple une incohérence certaine dans le contexte des articles 12 et 13 du projet de loi sous avis.

Le fait d'omettre de notifier un traitement à la Commission nationale n'est puni que d'une amende de 10.001 à 1.000.000 de francs, alors que le fait d'informer la même institution, même si c'est de façon incomplète ou inexacte, entraîne un emprisonnement de 8 jours à 6 mois et/ou une amende de 10.001 à 3.000.000 de francs. Par contre, le fait de mettre en œuvre un traitement modifiant la pratique en cours avant d'en avoir informé la même Commission nationale n'est de nouveau passible que d'une amende de 10.001 à 3.000.000 de francs.

Dans les conditions données, le Conseil d'Etat donne à considérer s'il ne serait pas autrement judicieux de sanctionner uniformément tous les comportements jugés répréhensibles par une même peine pénale correspondant (par exemple) à un emprisonnement de 8 jours à un an et à une amende de 10.001 à 5.000.000 de francs[1], ou à l'une de ces peines seulement. Il appartiendra toujours aux cours et tribunaux d'adapter la sanction à la gravité de la faute en puisant la peine correctionnelle à l'intérieur de la fourchette prévue et sans préjudice de l'application de circonstances atténuantes.

Quant aux sanctions administratives

Comme précédemment relevé, l'ampleur des sanctions administratives inscrites à l'article 35 du projet de loi sous avis est considérable. Placées dans leur contexte, ces mesures de répression ne manquent pas de soulever une critique fondamentale en rapport avec la nature de ces sanctions dites „administratives".

Le maximum de l'amende d'ordre, soit 10.000.000 de francs, correspond au double du maximum de l'amende correctionnelle. En cas de récidive sanctionnée par la Commission nationale, elle peut même monter jusqu'au quadruple de l'amende pénale. De par son envergure, cette amende d'ordre ne peut donc plus guère être taxée d'administrative, mais prend plutôt le caractère d'une sanction pénale avec toutes les conséquences que comporte ce rapprochement quant aux garanties exigées en la matière par la Convention européenne des droits de l'homme. Ainsi un recours de pleine juridiction devrait être prévu en l'occurrence.

Aussi le Conseil d'Etat propose-t-il d'exclure les amendes d'ordre de l'arsenal mis à la disposition de la Commission nationale pour sanctionner les „infractions commises à la (présente) loi et/ou à ses règlements d'exécution ainsi qu'aux instructions de la Commission". L'article 35 tel que prévu au projet ne respecte en effet guère le principe fondamental de la légalité des délits et des peines qui en exige une détermination précise afin d'assurer la prévisibilité des sanctions attachées à un comportement précis. En outre, il convient de maintenir les sanctions à caractère pénal sous l'égide des tribunaux de l'ordre judiciaire, garants naturels des libertés publiques[2].

---

1 A adapter conformément au chapitre II de la loi du 19 août 2001 relative au basculement en euro le 1er janvier 2002 et modifiant certaines dispositions légales

2 Rapport de la Commission juridique de la Chambre des députés sur le projet de loi portant modification de la loi modifiée du 18 mars 1972 … (Doc. parl. No 4013^5, sess. ord. 1994-1995)

Même à supposer que les amendes d'ordre prévues en l'espèce fussent de nature administrative, les réserves juridiques n'en seraient pas pour autant écartées. Surgirait en effet alors la question de la légitimité du cumul de sanctions administratives et pénales pour réprimander un même fait. En principe, un tel cumul ne peut être admis que dans trois cas:

– il est possible d'admettre des sanctions administratives ayant un caractère provisoire, en attendant l'intervention d'une sanction pénale;
– le cumul se justifie également lorsque les deux sanctions n'ont pas la même nature;
– le cumul peut encore se justifier lorsque la sanction pénale est regardée comme une arme d'emploi exceptionnel.[1]

Le Conseil d'Etat estime qu'aucune des trois hypothèses n'est donnée en l'espèce.

Mieux vaut donc s'en tenir aux prescriptions de la directive qui prévoit sous le deuxième tiret du paragraphe 3 de son article 28 que l'autorité de contrôle doit être pourvue „de pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en œuvre des traitements, conformément à l'article 20, et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui *d'adresser un avertissement ou une admonestation au responsable du traitement* ou celui de saisir les parlements nationaux ou d'autres institutions politiques". Aux instances administratives incombe ainsi un rôle régulateur et correcteur, alors que le volet répressif doit être réservé aux autorités pénales.

*

EXAMEN DES ARTICLES

Article 1er

En vertu de l'article 1er de la directive, les Etats membres sont obligés d'assurer „la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel". Au sens dudit acte communautaire, la vie privée mérite protection en tant qu'élément rentrant, parmi d'autres, dans la définition même des libertés et droits fondamentaux.

Le projet de loi sous avis se propose par contre de protéger la vie privée „ainsi que" les libertés et les droits fondamentaux des personnes physiques. Par sa formulation, il suggère qu'il y aurait juxtaposition de deux catégories d'intérêts à préserver au même titre. Le Conseil d'Etat préférerait dans ce contexte s'en tenir à l'approche de la directive.

Le texte sous examen entend encore faire respecter „les intérêts légalement protégés" des personnes morales. Selon son commentaire, „la référence à l'intérêt légalement protégé (…) permet de prévenir l'utilisation de certains droits tirés de la présente loi à des fins illégitimes". De l'avis du Conseil d'Etat, la référence à la légitimité des intérêts d'une personne morale serait autrement pertinente que la mention de ses intérêts légalement protégés.

En conclusion des développements qui précèdent, l'article 1er s'énoncera comme suit:

„**Art. 1er. –** ***Objet***

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 et fait respecter les intérêts légitimes des personnes morales."

Il convient de signaler qu'en étendant ainsi la protection aux personnes morales, l'article 1er, tant dans sa teneur initiale que dans la version proposée par le Conseil d'Etat, va au-delà du champ d'application et de la directive 95/46/CE et de la Convention de Strasbourg qui est limité aux personnes physiques.

Il y a lieu de préciser en outre d'emblée que la loi en cours d'élaboration s'appliquera indistinctement aux secteurs public et privé, restant en cela conforme avec l'article 3, paragraphe 1er de ladite Conven-

---

1 Voir „Les conditions du cumul entre sanctions administratives et sanctions pénales" in „Les pouvoirs de l'administration dans le domaine des sanctions", étude adoptée par l'Assemblée générale du Conseil d'Etat français, le 8 décembre 1994

tion du Conseil de l'Europe du 28 janvier 1981. Dans cette optique, le Conseil d'Etat est cependant à se demander si l'ensemble des dispositions visées peut, tel quel et sans autre forme d'aménagement, s'appliquer au secteur public.

Article 2

Cet article réunit les définitions essentielles traversant le projet.[1] S'y ajoutent deux notions déterminées au paragraphe 1er de l'article 6, à savoir celles de „donnée relative à la santé" et de „donnée génétique". Le Conseil d'Etat propose de transférer ces dernières à l'article 2 sous la forme des lettres (q) et (r).

Les différentes définitions, reprises pour la plupart de la directive, appellent les observations suivantes.

La lettre (b) définit comme personne concernée „toute personne physique ou morale, publique ou privée ou groupement de fait sujet d'un traitement de données à caractère personnel". Le groupement de fait n'a pas sa place en l'espèce et le Conseil d'Etat propose partant de l'omettre. Il n'est en effet pas spécialement évoqué à l'article 1er énumérant les personnes à protéger. Par ailleurs, un tel groupement de fait réunit toujours des personnes soit physiques soit morales, de sorte que son énonciation sous la lettre (b) n'ajoute rien à la portée du projet de loi sous revue.

Toujours dans le même contexte, le Conseil d'Etat s'interroge encore sur la signification exacte de la précision „sujet d'un traitement de données à caractère personnel". Se rapporte-t-elle au groupement, comme le fait présumer l'accord? Vise-t-elle en outre les personnes physiques ou morales, publiques ou privées figurant également sous la lettre (b)? Ou les auteurs n'ont-ils pas plutôt voulu entendre par „personne concernée" celle faisant l'*objet* d'un traitement de données à caractère personnel?

Selon son commentaire, la définition en cause „précise que la loi vise le respect des libertés et droits fondamentaux des personnes physiques, mais également, le cas échéant, le respect des intérêts légitimes[2] des personnes morales, publiques ou privées, et des groupements de fait". Au regard des droits accordés à la personne concernée par les dispositions inscrites au Chapitre VI du projet de loi sous avis[3], le Conseil d'Etat estime qu'il y a lieu de remplacer le mot „sujet" par le terme „objet"[4].

La lettre (b) se lira par conséquent ainsi:

> *„(b) „personne concernée": toute personne physique ou morale, publique ou privée, qui fait l'objet d'un traitement de données à caractère personnel;"*

La lettre (h) cerne la notion de surveillance. Le commentaire est quelque peu osé en affirmant hardiment qu'il s'agit d' „une notion centrale dans le cadre de l'activité de prévention de la criminalité", alors que la recherche „pro-active" ne rentre justement pas dans le champ d'application du projet de loi sous avis!

Quant au texte, le Conseil d'Etat propose de le reformuler en ces termes:

> *„(h) „surveillance": 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;"*

La lettre (i) définit le sous-traitant dont les obligations sont déterminées à l'article 21.

Sous la lettre (k) est défini le „destinataire" de données. Ne sont pas à considérer comme tel „les autorités qui sont susceptibles de recevoir communication de données à caractère personnel *dans le cadre d'une mission d'enquête particulière*". Le texte du projet de loi ne définit pas autrement les autorités

---

1 Le projet de loi regroupe les définitions sous les lettres allant de (a) jusqu'à (r), sauf que la lettre (n) manque. Cette erreur doit être redressée et l'énonciation est à réagencer en conséquence

2 „intérêts légitimes", désignation confortant les observations et la proposition de texte du Conseil d'Etat au regard de l'article 1er ci-avant examiné

3 droit à l'information (art. 26 et 27), droit d'accès (art. 28 et 29), droit d'opposition (art. 30) et droit de ne pas être soumis à une décision automatisée (art. 31)

4 Ce n'est en effet pas la personne concernée qui joue un rôle actif en l'espèce et effectue le traitement de ces données. Elle n'est pas „sujet", mais „objet" en l'occurrence

visées, contrairement à son commentaire qui précise qu'„il s'agit, par exemple, des agents du fisc ou encore ceux de la sécurité sociale spécialement habilités pour opérer des contrôles sur les informations traitées. Ne seront pas considérées comme destinataires les autorités publiques dans le cadre de commissions rogatoires internationales".

Le Conseil d'Etat, dans le but de mieux traduire l'intention des auteurs de la disposition visée, propose de remplacer dans le cadre de la lettre (k) les termes „dans le cadre d'une mission d'enquête particulière" par ceux de *„dans le cadre de l'exécution d'une mission légale d'enquête ou de contrôle"*.

Au sens de l'article 2, h) de la directive, est considérée comme consentement de la personne concernée „toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement". La lettre (l) de l'article 2 du projet de loi sous revue prescrit que cette manifestation de volonté soit par ailleurs „non équivoque", tout en pouvant également émaner du „représentant légal, judiciaire ou statutaire" de la personne concernée. Le Conseil d'Etat se demande si, pour être qualifié de non équivoque, ce consentement ne doit pas en outre être exprès, adjectif d'ailleurs employé par l'article 11, paragraphe 1er, alinéa final, pour relever que dans le cadre d'un traitement mis en œuvre à des fins de surveillance sur le lieu de travail, même le consentement „exprès" de la personne concernée ne saurait légitimer une application contraire à la loi. Notons encore que le commentaire de la définition sub (l) se réfère aussi au caractère, entre autres, exprès que doit revêtir la manifestation de volonté pour valider le consentement de la part de la personne concernée. Dans les conditions données, il est proposé de conférer la teneur suivante à la lettre (l) de l'article 2:

„(l) „consentement de la personne concernée": toute manifestation de volonté expresse, non équivoque, 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;"

La lettre (m) définit le code de conduite correspondant à des „contributions sectorielles élaborées en vue de la bonne application de la (présente) loi". Le Conseil d'Etat n'entrevoit guère les contours, ni d'ailleurs l'utilité d'une telle définition au regard des obligations pesant sur les Etats membres en vertu de l'article 27 de la directive. Aussi propose-t-il d'éliminer de l'article 2 la définition de ce code.

Afin de prévenir tout risque de confusion – aussi minime fût-il – entre la Commission des Communautés européennes et la Commission nationale pour la protection des données, le Conseil d'Etat suggère de désigner cette dernière par „la Commission nationale" au lieu de „la Commission" et de redresser en conséquence la lettre (p) ((n) selon le Conseil d'Etat) de l'article 2. Cette nouvelle abréviation doit par ailleurs être répercutée à travers l'ensemble du projet sous avis.

La lettre (q) ((o) selon le Conseil d'Etat) considère comme instance médicale „toute personne physique ou morale autorisée à exercer, soit des activités ayant pour objet la prévention, le diagnostic ou le traitement de maladies et infirmités, soit des activités de soins, soumise au secret professionnel au sens de l'article 458 du code pénal". Il n'est pas sûr que cette formulation englobe toutes les professions de la santé. Le doute est permis notamment pour ce qui est des pharmaciens ou encore du personnel paramédical. Aussi le Conseil d'Etat propose-t-il d'écrire, par référence à l'article 8, paragraphe 3 de la directive:

„(o) „instance médicale": tout praticien de la santé ainsi que toute personne soumise à la même obligation de secret professionnel, 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;"

Cette définition est censée viser toutes les professions de la santé et tous les fournisseurs de soins de santé, pour autant toutefois qu'il s'agit de personnes physiques, seules soumises à l'article 458 du Code pénal.

Comme ci-avant annoncé, le Conseil d'Etat examine à cet endroit les définitions figurant sous les lettres (a) et (b) du paragraphe 1er de l'article 6 du projet de loi qu'il propose d'insérer à l'article 2 sous les lettres (q) „donnée relative à la santé" et (r) „donnée génétique".

De l'avis du Conseil d'Etat, il y a lieu d'inclure parmi les données relatives à la santé „les" données génétiques en général, et non seulement „certaines"[1] d'entre elles. Seraient par contre à en exclure „les informations sociales et administratives connexes susceptibles d'avoir une incidence" sur l'état physique et mental d'une personne[2], de sorte que la lettre (q) de l'article 2 prendrait la teneur suivante:

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

La lettre (r) est à rédiger comme suit:

„(r) „donnée génétique": toute donnée concernant les caractères héréditaires d'un individu ou d'un groupe d'individus apparentés."

Article 3

Au vœu du paragraphe 1er, la loi en élaboration a vocation à s'appliquer au traitement automatisé ou non de données contenues ou appelées à figurer „dans un fichier", structuré ou non, contrairement à la directive qui vise les seuls fichiers structurés[3].

Le paragraphe 2, lettre (a) peut être simplifié en écrivant:

„(a) par un responsable du traitement soumis au droit luxembourgeois", au lieu de:

„(a) par un responsable du traitement établi sur le territoire luxembourgeois ou en un lieu où, selon le droit international public[4], est applicable le droit luxembourgeois;"

Le libellé de la lettre (b) du paragraphe 2 est quelque peu maladroit. Aussi le Conseil d'Etat propose-t-il, dans le respect de la disposition inscrite au paragraphe 1er, sub c) de l'article 4 de la directive, la modification rédactionnelle suivante:

„(b) un responsable du traitement qui n'est pas établi sur le territoire de l'Union européenne, mais recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire luxembourgeois. Toutefois, si ces moyens ne sont utilisés qu'à des fins de simple transit sur le territoire luxembourgeois[5], le responsable du traitement désigne, par une déclaration écrite à la Commission nationale, un représentant établi sur le territoire luxembourgeois qui se substitue aux droits et obligations du responsable du traitement, sans que[6] ce dernier ne soit dégagé de son éventuelle responsabilité particulière."

Le paragraphe 3 de l'article 3, à l'encontre de ses paragraphes 1er, 2, 4 et 5 définissant les traitements auxquels s'appliquera la loi en préparation, détermine une hypothèse dans laquelle cette dernière ne s'appliquera précisément pas. La disposition mérite partant d'être recalée à la fin de l'article 3 pour y figurer comme paragraphe 4.

Le paragraphe 4 fait double emploi avec l'article 2, (a) et peut donc être radié de l'article 3.

Le paragraphe 5 (3 selon le Conseil d'Etat) appelle quelques amendements rédactionnels. Il est proposé d'évoquer dans le présent contexte le traitement de *données concernant* la sécurité publique … au lieu de parler simplement de „traitement ayant pour objet la sécurité publique …". Le texte du projet fait par ailleurs référence au „bien-être économique de l'Etat", notion quelque peu inadaptée en l'occurrence, raison pour laquelle le Conseil d'Etat propose d'y substituer la terminologie employée au considérant 43 de la directive.

Le paragraphe sous examen s'énonce en conséquence comme suit:

---

1 Resterait à savoir lesquelles?

2 C'est-à-dire?

3 Voir article 3, paragraphe 1er en relation avec l'article 2, c) de la directive

4 Pourquoi pas aussi le droit international privé?

5 La directive parle de transit sur le territoire de la Communauté!

6 Au regard de sa portée assez floue (cf. „éventuelle", „particulière"), l'on peut se demander si cette réserve mérite d'être maintenue.

„(3) La présente loi s'applique 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[1] des dispositions spécifiques de droit national ou international régissant ces domaines."

Article 4

D'après le paragraphe 1er, le responsable du traitement doit „garantir", entre autres, que les données qu'il traite le sont loyalement et licitement. De par sa formulation, cette obligation absolue risque de s'avérer illusoire. La directive est moins rigoureuse sous cet aspect en imposant par le paragraphe 2 de son article 6 au responsable du traitement le devoir d'„assurer" le respect des dispositions visées en son paragraphe 1er. Le Conseil d'Etat a, quant à lui, une préférence pour le verbe „s'assurer de ce que" évoquant davantage une obligation de moyens qu'une obligation de résultat et restant en cela plus proche des possibilités réelles de contrôle dont peut disposer en fait le responsable du traitement.

Dans cette optique plus réaliste des choses, le paragraphe 1er prend la teneur suivante:

„(1) Le responsable du traitement doit s'assurer de ce que les données qu'il traite le soient loyalement et licitement, et notamment que ces données soient:

(…)"

Au paragraphe 3, il y a lieu de remplacer les termes „de cet article" par les mots „du présent article". La même observation s'impose d'ailleurs à l'endroit des articles 5, paragraphe 2, (7, paragraphe 5), 8, paragraphe 4, 10, paragraphe 5, 14, paragraphe 3, 17, paragraphe 3, 26, paragraphe 4, 28, paragraphe 8 et 30, paragraphe 4.

Article 5

Cet article détermine les conditions de nature à garantir la légitimité d'un traitement de données.

Le Conseil d'Etat est à se demander si, au regard de la disposition inscrite sous la lettre (c) du paragraphe 1er, le commerce électronique ne tombe pas également dans le champ d'application de l'article 5 et sera partant soumis aux mêmes prescriptions de légitimité.

Si, dans l'intention des auteurs du projet de loi sous examen, cette question devait recevoir une réponse affirmative, il pourrait en surgir un problème de coexistence harmonieuse avec l'article 20[2] de la loi du 14 août 2000 relative au commerce électronique qui, contrairement au paragraphe 2 de l'article 5 sous revue, ne prévoit pas de sanction pénale pour un traitement violant ses dispositions légales.

Article 6

Tout comme l'article 8, paragraphe 1er de la directive, le paragraphe 1er inclut parmi les données sensibles celles relatives „à la vie sexuelle" dont les contours sont cependant loin d'être précis. Est-ce que ce ne serait pas plutôt l'orientation sexuelle des personnes concernées que leur vie sexuelle au sens large qui serait visée en l'occurrence?

Le paragraphe 1er énonce encore parmi les catégories méritant une protection particulière le traitement „*des*" données génétiques. Parmi les données relatives à la santé, le même texte n'évoque par contre sous a) que les traitements de „*certaines*" données y relatives. Il s'entend cependant que dans le cadre de l'application de la loi en élaboration, les données génétiques se définissent toujours par référence à la lettre (b), paragraphe 1er de l'article 6 (lettre r de l'article 2 selon le Conseil d'Etat).

A noter que les deux notions définies sous les lettres (a) et (b) de l'article 6 ont été transférées dans une forme légèrement modifiée par le Conseil d'Etat aux lettres (q) et (r) de l'article 2.

---

1 Le paragraphe correspondant du projet de loi sous examen décrit comme suit la réserve en question: „sans préjudice des dispositions spécifiques contenues dans les instruments de droit international qui lient le Grand-Duché de Luxembourg et des dispositions légales spécifiques dans ces domaines respectifs"

2 Ledit article 20 intitulé „De la protection des données à caractère personnel" prévoit en effet en un paragraphe 1er que „l'Autorité Nationale d'Accréditation et de Surveillance et les prestataires de service de notification sont tenus au respect des dispositions légales régissant le traitement de données à caractère personnel", sans en incriminer la violation par une disposition spécifique inscrite au Titre III (Dispositions pénales) de la loi du 14 août 2000

Le paragraphe 2 détaille les exceptions au principe d'interdiction du traitement de catégories particulières de données dites sensibles.

Ainsi, selon la disposition sous (a), ce traitement devient licite lorsque la personne concernée y a donné son consentement, à condition toutefois qu'aucune disposition légale ne s'y oppose et „sauf indisponibilité du corps humain". Le Conseil d'Etat a du mal à saisir la portée de cette dernière précision dans le présent contexte. Il peut certes être indiqué de passer outre l'absence de consentement de la personne concernée lorsqu'il s'agit de préserver les intérêts vitaux de la personne en cause, voire d'une tierce personne, mais uniquement dans cette hypothèse extrême, d'ailleurs prévue sous la lettre (c) du paragraphe 2 de l'article 6.

De l'avis du Conseil d'Etat, la disposition sous a) de l'article 6, paragraphe 1er est à reformuler comme suit:

> *„(a) la personne a donné son consentement exprès à un tel traitement, sauf le cas interdit par la loi, ou lorsque."*

Selon la disposition prévue sous (b), le même traitement est encore légitime dans la mesure où il permet au responsable du traitement de se mettre en conformité avec le droit du travail. Dans ce contexte, il est suggéré de substituer aux mots „par disposition légale" ceux de „par la loi" pour souligner qu'est ici visée la loi au sens large.

La dérogation figurant sous (c) est dictée par la nécessité de sauvegarder les intérêts vitaux d'une personne, notamment dans le cas de prélèvement de substances d'origine humaine régi par la loi du 25 novembre 1982.

Autre hypothèse justifiant la mise en échec de l'interdiction de traitement de données sensibles: lorsque le traitement est mis en œuvre, avec le consentement de la personne concernée, par les associations définies sous (d). Le Conseil d'Etat, tout en étant conscient que la disposition en cause est reprise de l'article 8, paragraphe 2 de la directive, a quelque appréhension à y voir figurer non seulement les données concernant les membres d'une telle association, mais également celles relatives aux tiers entretenant avec elle „des contacts réguliers liés à (sa) finalité", d'autant plus que les contours exacts de ces derniers sont loin d'être définis.

Le traitement est encore licite lorsque, selon (e), il porte sur des données „manifestement" rendues publiques par la personne en cause „ou dès que son consentement au traitement des données peut légitimement être déduit de ses déclarations". Il s'avérera sans doute difficile de distinguer les données *manifestement* rendues publiques des autres. Par ailleurs, il est inacceptable que le traitement de données sensibles puisse s'effectuer sur la base d'un consentement *déduit* à partir de *déclarations* faites par un individu dans des circonstances non autrement définies. L'article 8, paragraphe 2 de la directive ne prévoit pas pareille ouverture et le Conseil d'Etat préconise finalement d'éliminer l'hypothèse en question du texte figurant à l'article 6, paragraphe 2, sous (e).

Le même paragraphe 2 prévoit sous (f) qu'est en outre légitime le traitement de données sensibles lorsqu'il est nécessaire „à la constatation, à l'exercice ou à la défense d'un droit en justice". Le commentaire de la disposition en question donne comme exemple „une analyse du sperme, respectivement du sang, (qui) peut s'avérer nécessaire pour déterminer, en cas de doute, l'auteur d'un viol ou encore pour l'établissement d'un lien de filiation". Il laisse entrevoir que cette mesure dérogatoire au principe d'interdiction inscrit au paragraphe 1er de l'article 6 est susceptible de s'appliquer tant en matière pénale qu'en matière civile. Selon ses auteurs, elle se justifie partant aussi bien dans l'optique des droits de la défense que dans la perspective de la défense d'un droit. Le Conseil d'Etat estime par contre que le contexte et la terminologie employée font plutôt référence à un enjeu de nature civile, compte tenu du libellé du paragraphe 3.

Dans le cadre de la disposition consignée sous (g), le Conseil d'Etat propose de supprimer l'adjectif „important" alors que, sous réserve de l'autorisation préalable de la Commission nationale, le traitement de données sensibles, à des fins historiques, statistiques ou scientifiques, paraît suffisamment motivé s'il est tout court justifié par un intérêt public et s'il ne peut être réalisé sur la base de données rendues anonymes[1]. En outre, le mot „notamment" est à radier, par référence au contenu des articles 4, paragraphe 2 et 14, paragraphe 1er.

---

1 Voir article 14, paragraphe 1er sub (b) du projet sous examen

Le paragraphe 4 en rapport avec les données génétiques fait encore état sous la lettre (b) de la notion d'„indisponibilité du corps humain", déjà évoquée sous le paragraphe 2 (a). Le Conseil d'Etat renvoie partant à son observation y relative.

Article 7

Le paragraphe 1er autorise, sous certaines conditions, le traitement de données sensibles au sens de l'article 6 lorsqu'il est mis en œuvre „par des instances médicales, ainsi que par les organismes de sécurité sociale et les administrations qui gèrent ces données en exécution de leurs missions légales et réglementaires". La question se pose s'il ne convient pas d'y inclure les entreprises d'assurance et les sociétés gérant les fonds de pension[1] ou encore certaines mutuelles.

Du point de vue formel, il y a lieu de remplacer par une virgule le point-virgule inséré en milieu du paragraphe entre le mot „médecine" et les termes „le traitement".

Au paragraphe 2, il se recommande d'écrire „le traitement visé *ci-dessus*" plutôt que „le traitement visé à *l'article 7 paragraphe (1)*".

Dans le contexte du paragraphe 4, il s'entend que la communication à des tiers de catégories particulières de données définies à l'article 6 ne peut se concevoir que dans la mesure où le traitement en lui-même de ces données est licite. Dans le but de souligner ce lien, le Conseil d'Etat propose de reformuler comme suit le paragraphe 4 de l'article 7:

> *„(4) 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."*

Au paragraphe 5, il est indiqué d'étendre l'incrimination pénale aux opérations illégales de communication de données à des tiers ou de leur utilisation illicite à des fins de recherche. La peine pénale ne doit donc pas s'appliquer au seul traitement illicite des données sensibles.

Pour éviter tout malentendu, le Conseil d'Etat propose d'introduire le paragraphe 5 par les termes *„quiconque effectue un traitement ou opère une communication à un tiers en violation des dispositions des articles 6 et 7"*, en remplacement de ceux de „quiconque effectue un traitement en violation de cet article[2]".

Article 8

Au vœu du paragraphe 1er, „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*". Cette dernière notion doit être entendue au sens large comme incluant les bases de nature réglementaire, par ailleurs visées à l'article 17.[3 et 4]

Le paragraphe 2 est à rédiger comme suit:

> *„(2) Il ne peut être tenu de recueil exhaustif des condamnations pénales que sous le contrôle de l'autorité publique compétente en la matière."*

Cette modification d'ordre rédactionnel n'affecte en rien la portée du texte original et continue de permettre la gestion d'un répertoire non exhaustif, ne visant donc que certaines condamnations pénales, par une autorité autre que judiciaire.

Le Conseil d'Etat estime trop restrictif le paragraphe 3 subordonnant le traitement de certaines données relatives aux jugements civils ou aux décisions administratives au contrôle de l'autorité publique (non autrement définie) compétente en la matière. Face au texte en cause, il faudrait en effet se

---

1 Voir la loi modifiée du 6 décembre 1991 sur le secteur des assurances et celle du 8 juin 1999 créant les fonds de pension

2 Lequel? L'article 6 ou l'article 7?

3 Elle permet ainsi de couvrir p.ex. le casier judiciaire, prévu à l'article 75 de la loi du 7 mars 1980 sur l'organisation judiciaire, mais organisé par le règlement grand-ducal du 14 décembre 1976 modifié par ceux des 27 avril 1984 et 8 février 1985

4 Exemples: – Le registre des contraventions ou délits en matière de circulation (Min. des Transports)
– La „chaîne pénale" Ingepol

demander si une administration déterminée pourrait, sans autre forme de procédure, continuer à gérer une banque de données documentaire. Dans les conditions données, le Conseil d'Etat propose d'éliminer le paragraphe 3 de l'article 8. La directive n'en sera pas moins respectée puisqu'elle dispose en son article 8, paragraphe 5, alinéa 2 que „les Etats membres *peuvent* prévoir que les données relatives aux sanctions administratives ou aux jugements civils sont également traitées sous le contrôle de l'autorité publique".

Le Conseil d'Etat s'interroge enfin sur le sort qui sera réservé aux banques existantes de données de l'espèce visée à l'article 8.

Article 9

Cet article a pour objet d'obtempérer à l'injonction inscrite à l'article 9 de la directive obligeant les Etats membres à prévoir „pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations au présent chapitre[1], au chapitre IV[2] et au chapitre VI[3] dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression".

Le législateur national se voit ainsi confronté au défi d'arbitrer entre deux libertés et droits fondamentaux essentiels: liberté d'expression et droit à la vie privée. Le dosage est des plus délicats d'autant plus que la marge de manœuvre des Etats membres reste très importante.[4]

Le Conseil d'Etat suggère en l'occurrence de ne pas préjuger de la réforme en perspective de la loi sur la presse et préconise de rechercher dans ce contexte une solution équilibrée. Aussi propose-t-il de reporter à cette occasion l'examen de la mise en œuvre de l'article 9 précité de la directive.

Article 10

Le paragraphe 1er détermine les hypothèses légitimant le traitement de données à des fins de surveillance au sens de l'article 2, lettre (h).

Selon la disposition prévue sous la lettre (b), cette surveillance peut ainsi être opérée „aux abords ou dans tout lieu accessible ou non au public", à condition qu'elle soit nécessaire à la prévention, à la recherche, à la constatation et à la poursuite d'infractions pénales. Le texte en question établit donc manifestement un lien entre les traitements visés et une finalité répressive. Or l'article 17 prescrit que les traitements d'ordre général nécessaires à la prévention, à la recherche, à la constatation et à la poursuite des infractions pénales doivent faire l'objet d'un règlement grand-ducal. Afin de prévenir toute insécurité juridique, il y a lieu de distinguer autant que faire se peut les champs d'application respectifs des articles 10 et 17. L'article 10, (b) vise le traitement à des fins de surveillance. L'article 17 a par contre trait aux „traitements d'ordre général nécessaires à la prévention, à la recherche, à la constatation et à la poursuite des infractions pénales". Les données recueillies au cours du premier sont donc susceptibles d'un traitement ultérieur dans le cadre général de la politique pénale, mais ne le sont pas nécessairement. Le paragraphe 3 confirme clairement cette approche sous ses lettres (b) et (c).

Toujours est-il que le Conseil d'Etat estime que la surveillance visée à l'article 10 doit rester cantonnée aux seuls lieux accessibles au public, à l'exception de tous les autres. Il se demande d'ailleurs comment, dans un champ de surveillance plus large, suffire à l'obligation d'information des „personnes concernées" prescrite au paragraphe 2 en relation avec l'article 26.

Compte tenu en outre d'une légère adaptation rédactionnelle et de l'un ou l'autre ajout, le point (b) du paragraphe 1er s'énoncera donc comme suit:

> *„(b) aux abords ou dans tout lieu accessible au public, notamment dans les parkings couverts, les gares, aérogares et 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"*

---

1 Chapitre II: Conditions générales de licéité des traitements de données à caractère personnel

2 Chapitre IV: Transfert de données à caractère personnel vers des pays tiers

3 Chapitre VI: Autorité de contrôle et groupe de protection des personnes à l'égard du traitement des données à caractère personnel

4 Voir les points 47 et 48 de l'étude citée sous la note 4 p. 3

L'ajout de la référence à la nature du lieu est destiné à englober notamment les bâtiments administratifs parmi les sites à surveiller et répondre ainsi à une préoccupation qui est d'actualité.

D'après le texte sous examen, le traitement à des fins de surveillance est encore licite „(c) dans une résidence privée dont le responsable du traitement est la personne physique y domiciliée". Le Conseil d'Etat propose de limiter la portée de cette disposition aux lieux d'accès privé, c.-à-d. aux locaux privatifs, tout en visant indistinctement les domiciles appartenant aux personnes physiques ou morales. Dans cette optique, la lettre (c) du paragraphe 1er de l'article 10 prendra la teneur suivante:

„(c) aux lieux d'accès privé dont la personne physique ou morale y domiciliée est le responsable du traitement."

L'information des personnes concernées d'après les modalités fixées au paragraphe 2 doit être restreinte aux cas de surveillance des lieux d'accès public. Il semble en effet quelque peu curieux de prescrire une telle information à l'égard d'une personne ayant déjà donné son consentement exprès à un tel traitement. Il en paraît de même pour ce qui est de la surveillance de locaux privatifs qui par définition ne donnent pas de droit d'accès libre aux tiers, y compris forcément toute „personne concernée" au sens du texte sous avis. Il convient partant de restreindre l'obligation d'information aux opérations de surveillance effectuées dans les lieux accessibles au public. Dans cette optique, il y a lieu de préciser au paragraphe 2 *in fine* que la prescription y consignée ne s'applique que dans le cadre „de la mise en œuvre des traitements visés au paragraphe (1) *sous (b)*", tel que proposé par le Conseil d'Etat.

Au paragraphe 3 sous (a), par analogie à la proposition de texte du Conseil d'Etat au regard de l'article 6, paragraphe 1er sous (a), il y a lieu d'écrire „sauf le cas interdit par la loi" au lieu de „nonobstant des dispositions contraires de la loi".

Le paragraphe 4 dispose que le „traitement à des fins de surveillance exclusivement mis en œuvre pour la prévention des infractions pénales est soumis à l'obligation d'information excluant ainsi l'application de l'article 27, paragraphe 1er (d)". Il est à éliminer de l'article 10 en ce que de deux choses l'une: ou bien il fait double emploi avec l'hypothèse visée au paragraphe 1er sub (b) du même article, ou bien il recouvre le cas d'application visé à l'article 17. De toute façon, il fait double emploi, car il ne peut y avoir de troisième situation justifiant la mise en place d'un traitement à des fins de surveillance.

Il en découle que le paragraphe 4 est à éliminer de l'article 10, le paragraphe 5 subséquent avançant ainsi d'une unité.

Article 11

Cet article a trait au traitement de données à des fins de surveillance sur le lieu de travail. En dehors des considérations particulières ci-avant développées en rapport avec le présent objet, il y a lieu de rappeler que les dispositions concernées sont destinées à s'appliquer tant au secteur public qu'au secteur privé.[1]

Force est de constater cependant que ni le comité mixte d'entreprise ni, à titre subsidiaire, l'Inspection du travail et des mines ne sont compétents en matière de relations de travail dans le secteur public. Tel quel, l'article 11 du projet de loi sous examen ne pourra donc trouver application dans le secteur public.

Le Conseil d'Etat est partant à se demander s'il n'est pas indiqué d'approfondir la question en la plaçant dans un contexte plus général. En attendant, il recommande d'éliminer du projet de loi sous avis l'article 11 sous examen avec toute la problématique qu'il préfigure.[2]

Ce n'est donc qu'à titre tout à fait subsidiaire que sont présentées les observations ci-après.

---

1 Voir observations *in fine* sous article 1er

2 Spiros Simitis, dans son article „Quatre hypothèses et quatre dilemmes (Quelques propos sur l'état actuel de la protection des données personnelles des salariés)" préconise même l'adoption de directives sectorielles afin d'aboutir à une protection effective des données personnelles dans le cas des salariés (in Droit Social/No 1er janvier 2002, pages 88 à 92 et plus particulièrement pp. 90-91)

Le paragraphe 1er précise dans son alinéa 1 que le traitement à des fins de surveillance sur le lieu de travail n'est notamment possible que „(a) pour les besoins de sécurité et de santé des travailleurs" et „(d) pour le contrôle temporaire de production ou des prestations du travailleur en vue de mesurer son activité afin de déterminer sa rémunération".

L'alinéa 2 ajoute que dans ces hypothèses, le comité mixte d'entreprise „a *un* pouvoir de décision tel que défini à l'article 7 paragraphes (1) et (2) de la loi du 6 mai 1974 instituant des comités mixtes dans les entreprises du secteur privé et organisant la représentation des salariés dans les sociétés anonymes". Or ce pouvoir découle directement de la loi *modifiée* du 6 mai 1974 précitée[1], nul besoin de le rappeler dans le présent contexte.

L'alinéa 3 dispose que „le consentement exprès de la personne concernée ne rend pas légitime le traitement mis en œuvre par l'employeur". Cette disposition est superfétatoire au regard du libellé restrictif du paragraphe 1er qui n'admet le traitement à des fins de surveillance sur le lieu de travail que dans les hypothèses limitativement énoncées.

Le paragraphe 2 délimite le cercle des personnes appelées à recevoir des informations notamment au sujet „(b) de la ou des périodes pendant lesquelles la surveillance *sera* effectuée". Au regard des personnes y mentionnées, l'on doit conclure que seuls les traitements énumérés au paragraphe 1er sous (a) et (d) sont concernés. Sous la lettre (c), il y a lieu d'éliminer les termes „le cas échéant".

Article 12

Le traitement sous (d) du paragraphe 2 vise la procédure de mise en état.

Les paragraphes 3 et 4 réunissant les dispositions pénales sanctionnant l'obligation de notification de certains traitements à la Commission nationale paraissent quelque peu incohérents. Selon le paragraphe 3, quiconque ne se soumet aucunement à ladite obligation risque une amende de 10.001 à 1.000.000 de francs. Par contre, celui qui y répond, mais en fournissant „sciemment" des informations incomplètes ou inexactes, est, selon le paragraphe 4, passible d'un emprisonnement de huit jours à six mois et d'une amende de 10.001 à 3.000.000 de francs, ou d'une de ces peines seulement.

Il n'y a pas de commune mesure entre les deux approches, par rapport au premier délit la sanction du deuxième pouvant en effet paraître disproportionnée. Pour ces motifs, le Conseil d'Etat propose de fondre dans un seul paragraphe 3 les pénalités frappant également les deux cas de figure:

> *„(3) quiconque ne se soumet pas à l'obligation de notification prévue ou fournit des informations incomplètes ou inexactes est puni d'une amende de 10.001 à 3.000.000 LUF."*[2]

Article 13

La disposition pénale figurant au paragraphe 4, à rapprocher de celle proposée par le Conseil d'Etat au regard de l'article 12, est superflue et peut par conséquent être rayée telle quelle.

Conformément au paragraphe 5 (4 selon le Conseil d'Etat), un règlement grand-ducal est appelé à fixer le montant et les modalités de paiement d'une redevance. S'agissant en l'espèce d'une taxe rémunératoire, ce procédé est compatible avec l'article 99 de la Constitution. Dans les faits, il s'agira cependant de veiller à ce qu'elle ne soit pas prohibitive.

---

1 Article 7, paragraphes 1er et 2:

„Le comité mixte d'entreprise a compétence de décision en ce qui concerne:

1. l'introduction ou l'application d'installations techniques destinées à contrôler le comportement et les performances du travailleur à son poste de travail;
2. l'introduction ou la modification de mesures concernant la santé et la sécurité des travailleurs ainsi que la prévention des maladies professionnelles."

2 Voir note 1 p. 7

Article 14

Le paragraphe 1er énumère les cas soumis à l'autorisation préalable de la Commission nationale. Dans le cadre des traitements de données à des fins historiques ou scientifiques dont question sous (b), „la Commission vérifie en particulier si ces traitements ne peuvent être réalisés sur base de données rendues anonymes". Le Conseil d'Etat se demande à quelle fin est censé s'effectuer cet examen. Lorsque le traitement peut effectivement être opéré sur la base de données anonymisées, la Commission est-elle tenue de refuser son autorisation ou peut-elle au contraire émettre une décision conditionnelle d'accord? Il serait même concevable qu'en l'hypothèse une telle autorisation ne serait pas requise. L'intention du législateur mérite en tout cas d'être précisée en l'espèce.

Est en outre subordonné à l'autorisation préalable de la Commission nationale „(d) le traitement concernant le *crédit* et la *solvabilité* des personnes concernées". Quelles peuvent bien être les données en rapport avec ces deux notions à la fois floues et qui seraient d'ailleurs définies par qui? A défaut de précisions à ce sujet, le Conseil d'Etat se prononce en faveur de la suppression de la disposition reprise sous la lettre (d).

A l'endroit de la lettre (e), le Conseil d'Etat se doit de signaler ses plus vives appréhensions en ce qu'elle admet implicitement que „l'utilisation de données à caractère personnel à des fins autres que celles pour lesquelles elles ont été collectées" puisse être envisagée. Pareille approche est inadmissible et la disposition inscrite au paragraphe 1er sous (e) est à rayer en conséquence. A quoi servirait sinon le consentement de la personne concernée donné à une fin bien précise? L'utilisation visée ne serait donc à la limite acceptable que si l'autorisation de la Commission nationale était de nouveau subordonnée au consentement de la personne concernée.

Le paragraphe 2 appelle les observations ci-après. D'après l'article 12, paragraphe 1er, un traitement ne peut être mis en œuvre avant sa notification à la Commission nationale. L'article 14 ajoute dans son paragraphe 1er que les traitements y énoncés sont en outre soumis à l'autorisation de ladite commission. Cette idée se retrouve au paragraphe 2 qui, dans sa première phrase, dit que „l'autorisation n'est délivrée par la Commission qu'après examen préalable à la mise en œuvre des traitements visés au paragraphe (1)". Le Conseil d'Etat propose de substituer à cette formulation quelque peu maladroite le libellé suivant:

> *„(2) La mise en œuvre des traitements visés au paragraphe (1) est subordonnée à l'autorisation de la Commission nationale."*

En fait, l'on pourrait toutefois même faire abstraction de cette disposition spécifique, alors qu'il résulte clairement du paragraphe 1er que „sont soumis à l'autorisation *préalable* de la Commission" „les *traitements*" recensés par la suite.

Dans sa dernière phrase, le paragraphe 2 dispose que „l'autorisation à délivrer en matière de traitement à des fins de surveillance sur le lieu de travail est subordonnée à l'avis préalable de l'Inspection du Travail et des Mines". Cette procédure cadre mal avec l'article 11, paragraphe 2, qui ne reconnaît qu'un caractère subsidiaire au rôle à jouer en l'occurrence par ladite administration. Il s'en déduit que la dernière phrase du paragraphe 2 de l'article 14 est à supprimer.[1]

Compte tenu des développements qui précèdent, se pose la question du maintien du paragraphe 2 réduit à la disposition assez anodine, ne serait-ce parce que non sanctionnée, qui énonce que „l'examen préalable est effectué dès la réception de la notification".

Au paragraphe 3 (2 selon le Conseil d'Etat), il y a lieu d'écrire „du présent article" plutôt que „de cet article".

Article 15

Conformément aux paragraphes 1er et 2, les notifications effectuées et les autorisations accordées sont répertoriées dans un registre.

Suivant le paragraphe 4, „la Commission publie un rapport annuel qui *fait état* des notifications et autorisations". D'après le Conseil d'Etat, la commission ne doit pas ici se limiter à dresser la liste de ces

---

1 Voir en outre l'observation principale du Conseil d'Etat à l'endroit de l'article 11

actes, mais sa mission consiste bien plus à publier annuellement le rapport *sur l'état* des notifications et autorisations. Le paragraphe 4 est donc à corriger en ce sens.

Article 16

Cet article ouvre le délicat débat de l'interconnexion de données à caractère personnel. Dans la mesure où cette opération est prévue par un texte légal, elle ne pose pas problème. Il n'en est cependant plus de même lorsque cette interconnexion peut, en l'absence de base légale, être autorisée par la Commission nationale intervenant à la demande conjointe des responsables des traitements à relier. Une telle extension ne peut être envisagée qu'à condition d'être entourée de solides garanties.

Avant d'entrer dans cette discussion, le Conseil d'Etat propose d'abord un amendement rédactionnel à l'endroit du paragraphe 1er qui prend la teneur suivante:

> *„(1) L'interconnexion de données à caractère personnel qui n'est pas expressément prévue par un texte légal doit faire l'objet d'une autorisation de la Commission nationale, sur demande conjointe présentée par les responsables des traitements en cause.“*

Il s'entend que la notion de „texte légal“ recouvre toute norme incorporée en droit national, quelle qu'en soit la source.[1]

En fait, c'est le paragraphe 2 qui définit les conditions pouvant, en l'absence d'habilitation législative, justifier une interconnexion de données et qui soulève une série d'interrogations non résolues.

Que faut-il ainsi entendre par objectifs „statutaires“ ? En outre, la cause d'intérêt légitime dans le chef des responsables des traitements ne devrait-elle pas se recouvrir ou du moins se concilier avec celle des personnes concernées pour justifier une interconnexion? Cette interconnexion ne devrait pouvoir s'effectuer qu'en l'absence d'un conflit d'intérêt entre les différentes personnes concernées. Dans cette perspective, il y a lieu d'insérer à la suite de l'évocation d' „un intérêt légitime pour les responsables des traitements“ les termes „et pour les personnes concernées“. Le Conseil d'Etat se demande même s'il ne faudrait pas soumettre l'opération visée à l'accord de la personne concernée.

La mention au paragraphe 3 d'un règlement grand-ducal devant déterminer les modalités de mise en œuvre de l'interconnexion n'est pas appropriée. Il s'agit en effet d'une opération technique qu'il appartient à la Commission nationale d'autoriser ou non, dans le respect des dispositions prévues au paragraphe 2 qu'il s'agira de revoir dans l'optique ci-dessus.

Article 17

Afin d'en augmenter la lisibilité, ledit article est à restructurer en deux paragraphes.

Le premier reprend sous les lettres (a) et (b) les dispositions figurant sous les points 1 et 2 de l'alinéa 1 de l'article 17 du projet. Le deuxième comporte la disposition pénale inscrite sous le point 3 du texte originaire.

La disposition sous la lettre (a) du paragraphe 1er mérite d'être reconsidérée dans son ensemble. Il n'est en effet ni possible en pratique ni conforme au droit applicable que le Procureur d'Etat puisse sans façon être institué en tant que responsable de l'ensemble des traitements auxquels il y est fait référence. En effet, si les procureurs d'Etat exercent la direction de la Police judiciaire, il n'en résulte pas qu'ils puissent être considérés comme responsables de tous les traitements susceptibles d'être mis en œuvre par la Police ou les Douanes. Par ailleurs, il faut tenir compte du fait que l'Inspection générale de la police relève de l'autorité du ministre de l'Intérieur et non pas du procureur d'Etat.

Toujours dans le même contexte, le Conseil d'Etat renvoie à ses observations au regard de l'article 42 du projet de loi sous avis qu'il propose de compléter par un paragraphe (4) à l'effet d'empêcher un vide juridique en matière de banques de données pénales, en attendant la publication des mesures réglementaires prévues par le texte sous revue.

Au paragraphe 2, il faut remplacer le renvoi aux dispositions „de cet article“ par celui portant sur les dispositions „du présent article“.[2]

---

1 donc également le droit international intégré dans notre système juridique par la voie d'une loi d'approbation

2 Voir encore note 1 p. 7

Article 18

Cet article introduit le chapitre IV concernant les transferts de données vers des pays tiers, visés par les articles 25 et 26 de la directive 95/46. Ces flux extra-européens ne pouvaient rester en dehors du champ d'observation des autorités communautaires. „Dès lors (en effet) qu'un niveau uniforme de protection des données était assuré sur le territoire communautaire, restait alors la question des (nombreux) flux de données extra-européens. La directive ne pouvait se contenter de les ignorer: c'eût été la ruine immédiate des efforts entrepris au sein de l'Union européenne. Elle ne pouvait pas non plus limiter les flux de données aux seuls pays disposant de législations équivalentes à celles des Etats membres en cette matière, sans s'isoler de manière intenable."[1] La directive s'est évertuée à naviguer entre ces deux écueils. Que face à une problématique aussi ardue la solution adoptée ne fasse pas l'unanimité ne doit pas surprendre.

Quant au texte de l'article 18, le Conseil d'Etat, en se référant au paragraphe 1er de l'article 25 de la directive, propose d'introduire le paragraphe 1er par le texte suivant censé clarifier la portée de l'article 18:

> *„(1) Le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement après leur transfert ne peut avoir lieu que …"*

Article 19

Cet article réunit les dérogations au principe d'interdiction de transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article précédent.

Le Conseil d'Etat craint que les particuliers ne soient pas toujours en mesure de se prémunir contre des stipulations contractuelles – risquant de devenir en fait de simples clauses de style – permettant une telle dérogation. A cet égard, l'article 26 de la directive ne se révélera guère suffisamment protecteur des personnes concernées par des traitements impliquant des transferts vers des pays tiers. On ne peut que le regretter.

Au regard du texte même, le Conseil d'Etat suggère de s'en tenir en principe à la terminologie retenue par la directive et d'écrire au paragraphe 1er sous la lettre (e) que „le transfert soit nécessaire à la sauvegarde de *l'intérêt vital* de la personne concernée", au lieu d'y viser „la vie" de cette même personne.

Au paragraphe 3, il y a lieu de désigner par „pays tiers" l'„Etat non membre de l'Union européenne", le tout par application de la terminologie définie à l'article 2, lettre (o) ((m) selon le Conseil d'Etat) du projet de loi sous avis.

Le Conseil d'Etat se demande enfin s'il ne convient pas de sanctionner également les transferts effectués en violation des dispositions prévues au paragraphe 1er et de compléter à cette fin la disposition pénale figurant au paragraphe 4 de l'article 19.

A cette fin, le paragraphe 4 de l'article 19 s'énoncera comme suit:

> *„(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 10.001 à 5.000.000 LUF[2], ou d'une de ces peines seulement."*

Article 20

Au paragraphe 1er, il y a lieu de supprimer les termes „pour la protection des données", conformément à la proposition du Conseil d'Etat émise à l'endroit de l'article 2, lettre (p) ((n) selon le Conseil d'Etat).

Dans la même logique, il est indiqué d'ajouter au paragraphe 2 l'adjectif „nationale" au mot „Commission" et de remplacer par „pays tiers" la désignation d'un „Etat non membre de l'Union européenne".

---

1 „Les flux transfrontaliers de données à caractère personnel en droit européen", par Bénédicte Havelange et Anne-Christine Lacoste/J.T.D.E./livraison de décembre 2001

2 Voir note 1 p. 7

Article 21

L'intitulé „confidentialité des traitements" ne correspond guère au contenu dudit article qui dispose que tout traitement de données s'effectue „sur instruction du responsable du traitement" qui, en vertu de l'article 22, doit tout mettre en œuvre pour assurer la sécurité des traitements. Le même reproche peut – il est vrai – être adressé à l'article 16 de la directive dont l'article 21 sous revue constitue une copie fidèle. En fait, l'article 21 semble plutôt viser la consultation non autorisée de données.

Notons enfin qu'il y a lieu de séparer par une virgule la désignation „lui-même" des termes „et qui accède à des données".

Article 22

Au paragraphe 1er, il est prévu que les mesures techniques et d'organisation instituées pour assurer la protection des données traitées „font l'objet d'un examen annuel dont le résultat est communiqué à la Commission". La disposition en question ne détermine pas la personne en charge de cet examen. Logiquement il devrait s'agir du responsable du traitement. Aussi le Conseil d'Etat propose-t-il de remplacer la dernière phrase du paragraphe 1er de l'article 22 par le texte suivant:

> *„Ces mesures font l'objet d'un rapport annuel à soumettre par le responsable du traitement à la Commission nationale."*

Le paragraphe 2 précise qu'il incombe au responsable du traitement de veiller au respect des mesures de sécurité technique et d'organisation à mettre en œuvre. Le Conseil d'Etat se demande si la même obligation ne devrait pas également peser sur le sous-traitant. Dans cette optique, il s'indiquerait d'intercaler dans la dernière phrase, entre le mot „traitement" et la préposition „de", les termes „ainsi qu'au sous-traitant".

Compte tenu des observations ci-dessus, le paragraphe 3 s'avère superflu. L'obligation figurant sous la lettre (a) ne constitue en effet qu'une simple redite de l'article 21, celle inscrite sous la lettre (b) se trouvant quant à elle reprise au paragraphe 2 de l'article 22, dans sa version préconisée par le Conseil d'Etat.

Au paragraphe 4, le bout de phrase „aux fins de la conservation des preuves" pourrait sans dommage être supprimé alors qu'il ne rappelle qu'une évidence. Le Conseil d'Etat s'interroge d'ailleurs sur l'utilité et la finalité du paragraphe 4 en tant que tel, puisqu'il est difficilement concevable que „les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences relatives à la sécurité des traitements" puissent être consignés autrement que „par écrit".

Article 23

Au vœu de l'alinéa 2 du paragraphe 1er de l'article 17 de la directive, les mesures de sécurité „doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger".

La formule introductive suivante de l'article 23 du projet de loi sous examen devrait, de l'avis du Conseil d'Etat, mieux traduire l'esprit de la directive:

> *„En fonction[1] 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:"*

Article 24

Au paragraphe 1er, il est dit que les personnes soumises au respect du secret professionnel prévu à l'article 458 du Code pénal, membres de la Commission nationale, le restent „même après la fin de leur mandat". Il s'agit d'un simple rappel d'une règle de droit commun. Le Conseil d'Etat estime que ce rappel n'est pas indispensable et propose partant d'en éliminer la mention dans le présent contexte.

Au paragraphe 3, la loi du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive

1 les termes „en fonction du" remplaçant ceux de „compte tenu du"

1999/93/CE du 13 décembre 1999 relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, la directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE du 20 mai 1997 concernant la vente à distance des biens et des services autres que les services financiers, peut être citée sous sa forme abrégée de „loi du 14 août 2000 relative au commerce électronique".[1]

Le paragraphe 4 dispose que „le responsable du traitement agissant dans le cadre de l'accomplissement de ses missions tel que visé à l'article 7 paragraphe (1), ne peut opposer à la Commission le secret professionnel auquel il est soumis". Rappelons que ledit article 7, paragraphe 1er, vise le domaine particulièrement sensible du traitement de données relatives à la santé. Or, dans ce contexte, la mainlevée du secret professionnel, même à l'égard de la Commission nationale, est inacceptable, du moins de par son caractère absolu. Aussi le Conseil d'Etat s'y oppose-t-il. Une dérogation au droit commun ne pourrait en effet se concevoir que dans la mesure où elle serait limitée aux renseignements concernant le volet technique du traitement de ces données sensibles. A cette fin, le paragraphe 4 de l'article 24 serait à compléter par la réserve suivante:

„ , pour autant que les renseignements demandés concernent les mesures visées à l'article 22, paragraphe (1)."

Article 25

Sans observation.[2]

Article 26

Cet article règle le droit à l'information de la personne concernée en distinguant selon que les données ont ou non été collectées directement auprès de cette dernière.

Les deux premiers paragraphes concernent l'hypothèse d'une collecte directe auprès de la personne concernée.

Le paragraphe 2 vise la collecte par voie de formulaire ou de questionnaire tout en l'assujettissant aux mêmes contraintes que celles frappant en général toute collecte directe. Il ne paraît partant ni nécessaire ni indiqué de prévoir une disposition spéciale concernant ce procédé particulier de rassemblement de données. Aussi le paragraphe 2 peut-il être supprimé. A la limite, parallèlement le paragraphe 1er pourrait être complété par le texte suivant à intercaler avant la première virgule[3]:

„ , quels que soient les moyens et supports employés,"

Le paragraphe 3 (2 selon le Conseil d'Etat) détaille les informations à fournir à la personne concernée afin de lui permettre d'exercer le cas échéant ses droits d'accès et d'opposition consacrés aux articles 28 et 30.

Au paragraphe 4 (3 selon le Conseil d'Etat), il y a lieu d'écrire „du présent article" au lieu de „de cet article".[4]

Article 27

Au paragraphe 1er, il convient de corriger la mention du paragraphe 3 de l'article 26 par celle du paragraphe 2, conformément à la proposition du Conseil d'Etat à l'endroit dudit article 26.

Sous la lettre (b), il est suggéré d'accoler l'adjectif „nationale" au sujet „la défense".

La lettre (e) diverge de la disposition correspondante de l'article 13 de la directive en ce qu'elle invoque, à titre d'exception au droit d'information de la personne concernée, „en particulier" les do-

---

1 Conformément à l'article 72 de ladite loi du 14 août 2000

2 Sauf note 1 p. 7

3 Virgule introduisant la phrase suivante: „le responsable du traitement ou son représentant doit fournir à la personne concernée"

4 Voir en outre note 1 p. 7

maines monétaire, budgétaire et fiscal, alors que l'acte communautaire se contente de les inclure parmi ceux dans lesquels l'intérêt économique ou financier important d'un Etat membre ou de l'Union européenne peut prévaloir. Le Conseil d'Etat se demande si les auteurs du projet sous examen ont à dessein voulu nuancer de la sorte l'objectif sous-jacent à la disposition en question.

Autre exception au droit à l'information de la personne concernée, celle inscrite sous (f) et – quelque peu paradoxalement – justifiée par „la protection de la personne concernée ou des droits et libertés d'autrui".

Compte tenu des observations du Conseil d'Etat au regard de l'article 9 ci-avant, le paragraphe 2 est à supprimer.

Le paragraphe 3 (2 selon le Conseil d'Etat) concerne les traitements à finalité statistique, historique ou scientifique, qui, de l'avis du Conseil d'Etat, devraient, dans toute la mesure du possible, s'effectuer à partir de données anonymisées.[1]

Article 28

Il est proposé de remplacer le début du paragraphe 1er par la disposition ci-après:

> *„(1) Sur demande à introduire auprès du responsable du traitement ou de son représentant, la personne concernée ou ses ayants droit justifiant d'un intérêt légitime peuvent obtenir sans frais, à des intervalles raisonnables et sans délais excessifs:"*

Il est en effet sous-entendu que le demandeur doit prouver son identité. Par ailleurs, la précision que le droit d'accès doit s'exercer „sans contrainte" paraît tout aussi implicite.

L'amende pénale prévue au paragraphe 2 doit, à l'instar de toutes les autres figurant au projet de loi sous avis, être adaptée conformément au chapitre II de la loi du 1er août 2001 relative au basculement en euro le 1er janvier 2002 et modifiant certaines dispositions législatives.

Conformément au paragraphe 3, „le patient a un droit d'accès aux données le concernant et collectées par son médecin. Le droit d'accès peut être exercé par le patient lui-même ou par l'intermédiaire d'un médecin qu'il désigne. En cas d'incapacité de la personne concernée, le droit d'accès peut être exercé par ses ayants droit".

Il s'entend que ce droit d'accès ne peut s'exercer que dans le respect des dispositions légales régissant les droits des patients.[2]

Le paragraphe 4 est en rapport avec l'article 9 visant le traitement réalisé dans le cadre de la liberté d'expression dont le Conseil d'Etat a proposé de reporter la discussion en vue de la réforme en perspective de la loi sur la presse. Dans cette optique, la disposition énoncée audit paragraphe 4 est à supprimer.

Au paragraphe 5, il y a lieu de redresser une faute d'inadvertance et de supprimer l'article „la" de trop en rapport avec la destruction des données mentionnée en fin de phrase.

---

1 Voir développements sous l'article 14

2 Voir notamment:

– Article 40, alinéas 1 et 2 de la loi du 28 août 1998 sur les établissements hospitaliers:

> **Art. 40.–** Lors de son admission à l'hôpital ou à l'établissement hospitalier spécialisé, ainsi que pendant son séjour hospitalier le patient a, en vue de son consentement éclairé, droit à une information adéquate sur son état de santé ainsi que sur les traitements proposés.
>
> Il incombe au médecin traitant d'en informer le patient. Ces informations peuvent être complétées par les autres prestataires de soins dans le respect des règles déontologiques applicables.

– Article 51 du code de déontologie des professions de médecin et de médecin-dentiste, édicté par le Collège médical et approuvé par arrêté ministériel du 21 mai 1991:

> **Art. 51.–** Pour des raisons légitimes que le médecin apprécie en conscience, un malade peut être laissé dans l'ignorance d'un diagnostic ou d'un diagnostic grave.
>
> Un pronostic fatal ne doit être révélé qu'avec la plus grande circonspection, mais les proches doivent généralement être prévenus, à moins que le malade n'ait préalablement interdit cette révélation ou désigné les tiers auxquels elle doit être faite.

Le Conseil d'Etat estime aussi utile de compléter ledit paragraphe 5 par l'ajout *in fine* du passage suivant:

„dans les conditions de l'article 35."

Au paragraphe 8, il se recommande de remplacer les termes „de cet article" par ceux de „du présent article".[1]

Article 29

Cet article détermine les exceptions et limitations au droit d'accès de la personne concernée garanti par l'article 28. D'après son commentaire, ces dérogations sont reprises de l'article 13 de la directive.

Il se trouve cependant que le paragraphe 1er ne reprend pas l'hypothèse visée à la lettre f) dudit article 13 justifiant la limitation du droit d'accès lorsqu'elle constitue une mesure nécessaire pour sauvegarder „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)[2];". Le commentaire est muet sur cette omission qui peut partant s'interpréter comme volontaire ou involontaire. Cette question mérite sans doute d'être clarifiée avant l'aboutissement de la procédure législative.

Les cas d'exception repris sous les lettres (e) et (f) du même paragraphe 1er se recouvrent avec ceux figurant sous les lettres (e) et (f) de l'article 27. Ils commandent en conséquence les mêmes observations que celles émises par le Conseil d'Etat à l'endroit dudit article 27.

Dans la suite de la proposition du Conseil d'Etat au regard des articles 9 et 28, paragraphe 4 ci-avant, l'hypothèse visée sous la lettre (g) du paragraphe 1er de l'article 29 sous revue est à supprimer.

Aux paragraphes 3 et 4, il convient d'écrire „Commission nationale" au lieu de „Commission", conformément à l'observation ci-avant au regard de la lettre (p) ((n) selon le Conseil d'Etat) de l'article 2.

Au paragraphe 5, il y a lieu d'exprimer en euros la fourchette de l'amende pénale prévue.[3]

Article 30

Cet article mérite d'être réagencé comme suit.

Dans un paragraphe 1er, introduit par les mots „Toute personne concernée a le droit:", il y a lieu de regrouper sous forme de lettres (a), (b) et (c) les différents droits en cause énumérés aux points 1 à 3 du projet.

La disposition pénale prévue au point 4 est à transposer au paragraphe 2 nouveau.

Conformément au point 2 ((b) selon le Conseil d'Etat), toute personne a le droit „de s'opposer, sur demande et gratuitement, au traitement la concernant envisagé par le responsable du traitement 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;". Les violations de cette disposition sont, en application du point 4 (paragraphe 2 selon le Conseil d'Etat), passibles „d'un emprisonnement de huit jours à un an et d'une amende de 10.001 à 3.000.000 LUF ou d'une de ces peines seulement".

Ces dispositions sont à rapprocher de l'article 48 (intitulé: „Des communications commerciales non sollicitées") de la loi du 14 août 2000 relative au commerce électronique qui s'énonce comme suit:

> „(1) La communication commerciale non sollicitée par courrier électronique doit être identifiée en tant que telle, d'une manière claire et non équivoque, dès sa réception par le destinataire.
>
> (2) L'envoi de communications commerciales par courrier électronique par un prestataire de service de la société de l'information à un destinataire n'est possible qu'en cas d'absence d'opposition manifeste de sa part.

---

1 Voir en outre note 1 p. 7

2 c) sécurité publique
d) intérêt économique ou financier important
e) prévention, recherche, constatation et poursuite d'infractions pénales ou de manquements à la déontologie

3 Voir note 1 p. 7

(3) Les prestataires qui envoient par courrier électronique des communications commerciales non sollicitées doivent consulter régulièrement les registres „*opt out*“ désignés par règlement grand-ducal où les personnes physiques qui ne souhaitent pas recevoir ce type de communications peuvent s'inscrire, et respectent le souhait de ces personnes. L'inscription des personnes physiques sur un ou plusieurs registres *d'opt out* se fait sans frais pour ces personnes.

Est puni d'une amende de dix mille un à deux cent mille francs, tout prestataire n'ayant pas respecté le souhait des personnes inscrites sur un ou plusieurs registres *d'opt out.*“

La juxtaposition des textes précités fait ressortir que tout en recouvrant sensiblement le même domaine – qui est celui de la prospection commerciale par voie électronique – ils divergent de façon radicale quant à l'échelle des sanctions pénales prévues. Cette situation ne manquera pas de provoquer quelques difficultés d'application. Aussi le Conseil d'Etat préconise-t-il, plutôt que d'harmoniser les dispositions pénales concurrentes, d'omettre le point 2 ((b) selon le Conseil d'Etat) de l'article 30 du projet de loi sous avis faisant, dans une large mesure du moins, double emploi avec l'article 48 de la loi précitée du 14 août 2000.

Au point 4 (paragraphe 2 selon le Conseil d'Etat) du texte du projet de loi sous revue, il y a lieu d'écrire „du présent article“ au lieu de „de cet article“.[1]

Article 31

Selon le paragraphe 1er, toute personne a le droit de ne pas être soumise aux décisions individuelles automatisées lorsque le traitement est „destiné à évaluer certains aspects de sa personnalité“. D'après le commentaire, „de telles décisions individualisées visent par exemple l'appréciation du rendement de la personne concernée, l'évaluation de son crédit, l'appréciation de sa personnalité et l'analyse de sa personnalité“. L'article 15 de la directive évoque, quant à lui, parmi les aspects de la personnalité d'un individu „son rendement professionnel, son crédit, sa fiabilité, son comportement“.

Reste que le texte de l'article 31, paragraphe 1er, est en lui-même passablement vague, de sorte qu'il pourrait être abandonné sans dommage. Dans cette optique, le paragraphe 2, devenant le paragraphe 1er, serait à reformuler comme suit:

„(1) Une personne peut être soumise à une décision individuelle automatisée produisant des effets juridiques à son égard, si cette décision:

a) …

b) …“

Article 32

Sans observation, sauf qu'il y a lieu d'écrire „Commission nationale“ en remplacement de „Commission“.

Article 33

Cet article institue une procédure d'urgence à actionner devant la chambre du conseil du tribunal d'arrondissement compétent, pour mettre fin à un traitement de données mis en œuvre en violation des prescriptions légales concernant la publicité, ou encore la procédure de notification ou d'autorisation. D'après le commentaire de l'article 33 en cause, cette procédure n'a vocation à se substituer, ni aux sanctions administratives que peut administrer la Commission nationale sur la base de l'article 35, ni aux procédures des référés de droit commun. En fait, „on s'est inspiré de la procédure d'urgence prévue dans la réglementation sur la profession de transporteur“.

Cet instrument procédural qualifié par les auteurs du projet de loi sous examen d'„efficace combinant rapidité et caractère semi-inquisitorial“, s'il est effectivement largement conforme aux dispositions de l'article 18 de la loi du 3 octobre 1991 concernant l'établissement de transporteur de voyageurs et de transporteur de marchandises par route, n'en demeure pas moins critiquable dans le présent contexte.

Il coexiste d'abord avec différentes procédures administratives et pénales, comme le relève d'ailleurs le commentaire. Cette juxtaposition de voies de droit sera source de conflits redoutables. Quelque louables que puissent donc avoir été en l'occurrence les intentions des auteurs du projet, le risque de les voir

1 Voir en outre note 1 p. 7

déjouées en pratique, à cause précisément de leur caractère illusoire, n'est pas négligeable. A cela s'ajoute que ce n'est pas en multipliant les sanctions et les recours que la protection des personnes concernées par le traitement de données à caractère personnel s'en trouvera nécessairement renforcée.

Tout compte fait, le Conseil d'Etat préconise donc l'élimination de l'article 33 du projet de loi sous revue. En ordre subsidiaire, il se propose d'émettre les observations suivantes au regard du texte visé.

Comme la chambre du conseil n'a pas d'audience fixe, les dispositions inscrites au paragraphe 2 quant à la notification et aux indications de la requête semblent quelque peu irréalistes.

Pour garantir un effet utile au paragraphe 3, il y a lieu de compléter les termes „entendus en leurs explications orales" par ceux de „ou dûment appelés".

Le Conseil d'Etat s'interroge en outre sur l'utilité et l'intérêt de l'alinéa 3 du paragraphe 9 qui prévoit que „les formalités du présent paragraphe sont à observer *sous peine de nullité*, sauf si la personne responsable du traitement, la partie civile, la Commission ou toutes les parties en cause y ont renoncé". Pourquoi vouloir assortir la violation de ces formalités par une nullité? Quelles seraient d'ailleurs ces formalités autres que l'observation du délai de convocation? En outre, quelles seraient ces „autres parties en cause"?

Article 34

Au paragraphe 1er, il y a lieu de supprimer l'indication que la Commission nationale pour la protection des données est „dénommée dans la présente loi „la Commission"[1]", précision qui fait double emploi avec la lettre (p) ((n) selon le Conseil d'Etat) de l'article 2. Pour rester par ailleurs conforme avec la même référence, il y a lieu d'écrire en lettres minuscules le titre complet de l'autorité de contrôle en cause.

Comme il s'agit en l'espèce d'une autorité non juridictionnelle, la disposition figurant sous la lettre (e) du paragraphe 3 peut être maintenue sous réserve d'être adaptée. Ainsi la Commission nationale ne saurait-elle tenir en échec le pouvoir réglementaire en omettant d'émettre son „avis préalable à l'adoption des mesures réglementaires" requis par la future loi. Elle ne saurait pas non plus paralyser l'action administrative en agissant de même dans le contexte des mesures administratives individuelles à prendre. Dans cette optique, la Commission nationale ne doit pas en l'occurrence aviser préalablement toutes les mesures réglementaires ou administratives, mais il est au contraire nécessaire et suffisant qu'elle soit consultée au préalable.

Toujours dans le contexte de la lettre (e) du paragraphe 3, le Conseil d'Etat estime qu'il est superfétatoire de préciser que la Commission nationale ne doit pas seulement être mise en intervention dans le cadre de l'adoption de mesures légales, réglementaires ou administratives, mais également en cas de modification de ces mêmes mesures. Cette règle découle en effet implicitement mais nécessairement de la solution de principe retenue. Il n'y a pas lieu d'insister. Quant à la publication des avis[2] de ladite commission, le paragraphe 3 (e) décide de recourir tant aux documents parlementaires qu'au rapport de la commission. D'après le Conseil d'Etat, il y a lieu de réserver la publication par la voie des documents parlementaires aux seuls projets et propositions de loi.[3]

Dans la logique des développements qui précèdent, le paragraphe 3, lettre (e), prendra la teneur suivante:

> *„(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 la base de la présente loi. Ces avis sont publiés au rapport annuel visé à l'article 15, paragraphe (4).*"

Au paragraphe 4, le Conseil d'Etat a du mal à concevoir ce qu'il faut entendre dans ce contexte par „une association … représentant" la personne (concernée) et qui aurait droit de saisir la Commission nationale d'une demande d'éclaircissement au sujet d'un traitement déterminé. S'agirait-il d'une asso-

---

1 Commission „nationale" selon le Conseil d'Etat (cf. observations sous la lettre (p) de l'article 2)

2 Le texte du projet parle d'avis en général. L'on peut partant admettre qu'il ne vise pas les seuls avis sur les projets ou propositions de loi ou encore les projets de règlement grand-ducal

3 Par application du droit commun

ciation dûment mandatée à cet effet? D'une association dont le principal intéressé serait simplement membre? Pourquoi le mandataire ne pourrait-il pas être tout aussi bien une personne physique? Pour lever cette équivoque, le Conseil d'Etat se demande s'il ne convient pas de substituer aux termes „ou par une association la représentant" les mots „*agissant par elle-même, par l'entremise de son avocat ou par toute autre personne physique ou morale dûment mandatée*".

Le paragraphe 5 requiert à son tour une observation. Il paraît en effet inadmissible que „la Commission peut, en particulier, être saisie par *toute personne* d'une demande de vérification de la liciéité d'un traitement en cas de refus ou de limitation de l'exercice du droit d'accès de la *personne concernée* conformément à l'article 29 paragraphe (4) de la présente loi".

L'adage „nul ne plaide par procureur" n'aurait-il plus cours? Le Conseil d'Etat se prononce en tout cas contre une aussi large ouverture du droit de saisine de la commission et propose de supprimer le paragraphe 5 de l'article 34.

Au paragraphe 6, il y a lieu de supprimer dans la phrase finale tout ce qui a trait à l'accès direct aux locaux où a lieu le traitement et qui risque d'être incompatible avec l'article 15 de la Constitution.

La disposition visée ne pourrait être maintenue qu'à condition qu'il soit précisé que seraient seuls visés les locaux „autres que d'habitation". L'accès aux locaux réservés à l'habitation ne devrait s'opérer que dans le respect des règles de droit commun (c.-à-d. flagrant délit ou mandat du juge d'instruction).

Le paragraphe 7 comporte manifestement un allégement de la condition de l'intérêt à agir, le tout en exécution de l'article 28, paragraphe 3, alinéa 1, 3e tiret de la directive.

Dans le cadre de l'application du paragraphe 8, la Commission nationale prendra soin de limiter la coopération avec les autorités de contrôle des autres Etats membres de l'Union européenne à l'échange des seules informations nécessaires à l'accomplissement de leurs missions en rapport avec l'exécution de la directive. Il faudra veiller à ce que cette collaboration s'opère dans les strictes limites du nécessaire et ne soit pas détournée de sa finalité primaire qui consiste à protéger les personnes à l'égard du traitement des données à caractère personnel.

Aux termes du paragraphe 9, „la Commission 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, de même qu'à toute autorité de contrôle commune instituée par des instruments juridiques internationaux".

De par son énoncé général, le paragraphe 9 substituant la Commission nationale à tout organe ou institution représentant le Grand-Duché de Luxembourg dans une autorité de contrôle commune fonctionnant dans le cadre des conventions ou accords internationaux liant notre pays est inacceptable. Quels sont en effet ces instruments juridiques visés?

Rappelons dans ce contexte que conformément à l'article 2 de la loi du 3 juillet 1992 portant approbation de l'Accord de Schengen[1], „le Procureur Général d'Etat est désigné comme autorité compétente conformément à l'article 57, paragraphe 3 de la Convention d'application".[2]

---

1 Loi du 3 juillet 1992 portant approbation – de l'Accord entre les Gouvernements des Etats de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, signé à Schengen, le 14 juin 1985 – de la Convention d'application de l'Accord de Schengen du 14 juin 1985, signée à Schengen, le 19 juin 1990 – des Protocoles d'adhésion de la République italienne, du Royaume d'Espagne et de la République portugaise à l'Accord du 14 juin 1985 – des Accords d'adhésion de la République italienne, du Royaume d'Espagne et de la République portugaise à la Convention du 19 juin 1990

2 Article 57:

1. Lorsqu'une personne est accusée d'une infraction par une Partie Contractante et que les autorités compétentes de cette Partie Contractante ont des raisons de croire que l'accusation concerne les mêmes faits que ceux pour lesquels elle a déjà été définitivement jugée par une autre Partie Contractante, ces autorités demanderont, si elles l'estiment nécessaire, les renseignements pertinents aux autorités compétentes de la Partie Contractante sur le territoire de laquelle une décision a déjà été rendue.

2. Les informations demandées seront données aussitôt que possible et seront prises en considération pour la suite à réserver à la procédure en cours.

3. Chaque Partie Contractante désignera, au moment de la ratification, de l'acceptation ou de l'approbation de la présente Convention, les autorités qui seront habilitées à demander et à recevoir les informations prévues au présent article.

Les dispositions précédentes ne font pas obstacle à l'application de dispositions nationales plus larges concernant l'effet „non bis in idem" attaché aux décisions judiciaires prises à l'étranger.

En vertu de l'article 2 de la loi du 29 mai 1998 portant approbation de la Convention Europol[1], „le service commun de la gendarmerie et de la police chargé de l'échange d'informations sur le plan international est désigné comme unité nationale chargée de l'exécution des fonctions énumérées à l'article 4 de la Convention"[2]. L'article 3 de la même loi du 29 mai 1998 pose que „l'autorité de contrôle prévue au paragraphe (4) de l'article 12-1 de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques est désignée comme l'autorité de contrôle nationale prévue à l'article 23 de la Convention[3] avec mission de contrôler le respect des dispositions en matière de protection des données à caractère personnel dans le cadre de l'exploitation du système d'information Europol".

Il convient donc non seulement de préciser les instruments juridiques visés, mais il s'impose en outre d'opérer la substitution envisagée dans les formes et selon les modalités prévues par les différents actes de droit international en cause afin qu'elle soit opposable aux autres Parties contractantes – à supposer

---

1 Loi du 29 mai 1998 portant approbation de la Convention sur la base de l'article K.3 du Traité sur l'Union européenne portant création d'un Office européen de police (Convention Europol), signée à Bruxelles, le 26 juillet 1995.

2 Article 4:

1. Chaque Etat membre crée ou désigne une unité nationale chargée d'exécuter les fonctions énumérées au présent article.

2. L'unité nationale est le seul organe de liaison entre Europol et les services nationaux compétents. Les relations entre l'unité nationale et les services compétents sont régies par le droit national, notamment par ses règles constitutionnelles.

3. Les Etats membres prennent toutes les mesures nécessaires pour assurer l'exécution des fonctions de l'unité nationale et, notamment, l'accès de cette unité aux données nationales appropriées.

4. Les unités nationales ont pour mission:

1) de fournir à Europol, de leur propre initiative, les informations et les renseignements qui sont nécessaires pour l'accomplissement de ses fonctions;
2) de répondre aux demandes d'informations, de renseignements et de conseils formulées par Europol;
3) de tenir à jour les informations et les renseignements;
4) d'exploiter et de diffuser dans le respect du droit national les informations et les renseignements au profit des services compétents;
5) d'adresser à Europol des demandes de conseils, d'informations, de renseignements et d'analyse;
6) de transmettre à Europol des informations à stocker dans les recueils informatisés;
7) de veiller au respect du droit lors de chaque échange d'informations entre Europol et elles.

5. Sans préjudice de l'exercice des responsabilités des Etats membres, telles qu'énoncées dans l'article K.2 paragraphe 2 du traité sur l'Union européenne, une unité nationale n'est pas tenue, dans un cas concret, de transmettre les informations et renseignements visés au paragraphe 4 points 1, 2 et 6, ainsi qu'aux articles 8 et 10, si la transmission:

1) porte atteinte à des intérêts nationaux essentiels en matière de sécurité,
2) compromet le succès d'enquêtes en cours ou la sécurité d'une personne ou
3) concerne des informations relevant de services ou d'activités spécifiques de renseignements en matière de sûreté de l'Etat.

6. Les frais exposés par les unités nationales pour la communication avec Europol sont à la charge des Etats membres et, à l'exception des frais de connexion, ne sont pas imputés à Europol.

Les Chefs d'unités nationales se réunissent en tant que de besoin pour assister Europol de leurs conseils.

3 Article 23:

1. Chaque Etat membre désigne une autorité de contrôle nationale chargée de contrôler en toute indépendance et dans le respect du droit national que l'introduction, la consultation ainsi que la transmission, sous quelque forme que ce soit, à Europol, de données à caractère personnel par cet Etat membre sont licites et de s'assurer que les droits des personnes n'en sont pas lésés. A cette fin, l'autorité de contrôle a accès, auprès des unités nationales ou des officiers de liaison, aux données introduites par l'Etat membre contenues dans le système d'informations et dans le système d'index selon les procédures nationales applicables.

Pour exercer leur contrôle, les autorités de contrôle nationales ont accès aux bureaux et aux dossiers des officiers de liaison respectifs au sein d'Europol.

En outre, conformément aux procédures nationales applicables, les autorités de contrôle nationales contrôlent les activités que mènent les unités nationales conformément à l'article 4 paragraphe 4 et celles des officiers de liaison conformément à l'article 5 paragraphe 3 points 1, 2 et 3 et paragraphes 4 et 5, dans la mesure où ces activités concernent la protection des données personnelles.

2. Toute personne a le droit de demander à l'autorité de contrôle nationale de s'assurer que l'introduction et la transmission à Europol, sous quelque forme que ce soit, des données qui la concernent ainsi que la consultation des données par l'Etat membre concerné sont licites.

Ce droit est régi par le droit national de l'Etat membre auquel appartient l'autorité de contrôle sollicitée.

qu'on soit vraiment attaché à cette solution. Il n'est cependant pas sûr que la Commission nationale soit dans tous les cas la mieux outillée ou la plus compétente pour remplir cette mission.

A moins que toutes les appréhensions ci-avant exprimées puissent être rencontrées de façon convaincante par une reformulation du paragraphe 9, le Conseil d'Etat propose de radier la proposition comparative introduite par la locution conjonctive „de même qu'à".

Au regard du paragraphe 10, le Conseil d'Etat se demande si l'ampleur des peines pénales prévues n'est pas quelque peu disproportionnée par rapport à la gravité des comportements à sanctionner.[1]

Article 35

Le paragraphe 1er prévoit qu'„une amende d'ordre qui ne peut dépasser 10.000.000 francs lorsqu'il s'agit d'une personne morale et (…) 500.000 francs lorsqu'il s'agit d'une personne physique" est susceptible de sanctionner l'une des infractions commises à la présente loi ou à ses règlements d'exécution ainsi qu'aux instructions de la Commission. En cas de récidive, le montant de l'amende d'ordre sera doublé.

De l'avis du Conseil d'Etat, ces amendes sont largement disproportionnées par rapport aux peines pénales par ailleurs inscrites au projet de loi. Elles risquent en outre de heurter le principe fondamental du „non bis in idem" en ce que et par leur envergure et par leur rapprochement de langage[2] ces amendes sont affectées d'un caractère quasi pénal.

Autres aspects critiquables:

Comment justifier que les mêmes faits soient sanctionnés différemment selon que l'auteur en est une personne morale ou physique?[3]

Pourquoi insister sur le doublement de l'amende d'ordre en cas de récidive, d'ailleurs non autrement spécifiée? A noter que la loi du 3 octobre 1991 concernant l'établissement de transporteur de voyageurs et de transporteur de marchandises par route[4] ne prévoit ni amende d'ordre ni forcément récidive.

En conclusion des développements ci-dessus, le Conseil d'Etat propose de supprimer le paragraphe 1er de l'article 35.

Au paragraphe 2, il y a lieu de supprimer en conséquence les mots „soit en sus de l'amende d'ordre" et de reformuler comme suit la disposition en cause:

> *„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 dans un ou plusieurs journaux quotidiens aux frais de la personne sanctionnée."*

Le Conseil d'Etat propose en outre d'instituer par un paragraphe nouveau un recours de pleine juridiction. Cette disposition pourrait prendre la teneur suivante:

> *„( ) 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."*

L'instauration d'un recours en réformation serait d'autant plus justifiée si, contrairement à l'avis du Conseil d'Etat, les amendes d'ordre prévues au paragraphe 1er étaient maintenues.

En ordre subsidiaire, – pour le cas où le paragraphe 1er dont question ci-avant serait maintenu – il faudrait clarifier les intentions des auteurs du projet de loi en la matière. Les sanctions disciplinaires

---

1 Abstraction faite de la nécessité de procéder à l'adaptation en euros de l'amende

2 Le texte parle d'„infraction" et de „récidive"

3 Deux poids et deux mesures pour les mêmes infractions?

4 Ci-avant évoquée sous l'article 33

prévues au paragraphe 2 doivent-elles s'ajouter systématiquement aux amendes d'ordre prononcées? Ou au contraire peuvent-elles le cas échéant accompagner ces sanctions pécunaires?

La locution adverbiale „en outre" plaiderait plutôt en faveur de la première thèse, n'y eût-il pas l'ajout de l'élément confondant „*soit* en sus de l'amende d'ordre" dans la même phrase introductive.

Le paragraphe 3 est à éliminer alors que la procédure administrative non contentieuse de droit commun s'applique d'office et garantit déjà „le respect du principe du contradictoire et des droits de la défense".

Si toutefois le paragraphe 3 visait la procédure contentieuse, ce serait au législateur et non pas au pouvoir réglementaire qu'incomberait la mission d'en déterminer les „modalités" de procédure.

Article 36

Même en l'absence d'une législation de base sur les établissements publics, il est généralement admis que l'établissement public:

– est créé par les pouvoirs publics, Etat ou communes, par la loi ou en vertu d'une loi, selon le principe que seul le législateur est compétent pour créer une personne publique;
– a une personnalité juridique distincte de l'Etat ou de la commune et jouit de l'autonomie administrative et financière;
– est créé en vue de la réalisation d'une mission spécifique déterminée par la loi;
– est placé sous la tutelle de l'Etat ou des communes.[1]

D'après l'article 36 sous examen, la Commission nationale pour la protection des données à créer prendra la forme d'un établissement public. La disposition en cause est censée mettre en œuvre l'article 28 de la directive qui prescrit en son paragraphe 1er que „chaque Etat membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les Etats membres en application de la (…) directive", avant d'ajouter que „ces autorités exercent en toute indépendance les missions dont elles sont investies".

Au paragraphe 1er de l'article 36 sous revue, il est dit que „la Commission est une autorité indépendante qui prend la forme d'un établissement public doté de la personnalité juridique, d'une autonomie administrative et financière. Son siège est établi à Luxembourg-Ville."

Selon les principes ci-avant rappelés, tout établissement public est soumis à la tutelle. En effet l'Etat, en consentant comme en l'espèce à la création d'un tel établissement, doit toujours pouvoir s'assurer que la personne juridique de droit public ainsi créée ne dépasse pas le cadre légal lui imparti et respecte la spécificité des missions lui attribuées. La Commission ne saurait donc se voir reconnaître le caractère d'une „autorité indépendante" au sens propre, tout en devant pouvoir, pour rester conforme avec la directive, „exercer en toute indépendance" les missions dont elle se trouve investie.

Dans cette optique, le Conseil d'Etat propose de libeller comme suit le paragraphe 1er de l'article 36 du projet de loi sous examen:

> *„(1) La Commission nationale est une autorité publique qui prend la forme d'un établissement public dont le siège est fixé à Luxembourg.*
>
> *Elle dispose de la personnalité juridique et jouit de l'autonomie financière et administrative, sous la tutelle du ministre ayant la protection des données dans ses attributions.*
>
> *Elle exerce[2] en toute indépendance les missions dont elle est investie en vertu de la présente loi."*

Sans dénaturer l'approche des auteurs du projet, le Conseil d'Etat propose de reformuler comme suit les paragraphes 2 et 3 de l'article 36:

> *„(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 Conseil de Gouvernement.*

---

1 Voir avis du Conseil d'Etat sur le projet de loi portant création d'un fonds national de la recherche dans le secteur public (Doc. parl. No 4438[1], sess. ord. 1998-1999)

2 Cf. dans le même sens article 37, paragraphe 8 du projet.

Le président et le vice-président sont désignés par le Grand-Duc.

Les membres sont nommés pour un terme de six ans, renouvelable une fois.

(3) Le Conseil de Gouvernement propose au Grand-Duc comme membres effectif et suppléant chaque fois au moins un juriste et un informaticien justifiant d'une formation universitaire accomplie."

Au paragraphe 2, le Conseil d'Etat a jugé utile d'insérer une disposition concernant la possibilité de révocation d'un membre de la Commission nationale.

Au paragraphe 3, il a estimé qu'il serait logique de prévoir que l'exigence de qualification dans le chef des membres effectifs doit se refléter au niveau des membres suppléants, permettant de remplacer ainsi en l'occurrence le membre par le suppléant justifiant de la même formation.

Le Conseil d'Etat a en outre jugé pouvoir se passer de l'alinéa 2 du paragraphe 3 tel que proposé par les auteurs du projet sous examen et disposant que:

„Les membres de la Commission sont proposés pour leur compétence professionnelle reconnue dans leur(s) matière(s) respective(s)."

Ne faut-il pas en effet admettre que cela va de soi?

Le paragraphe 6 définit le serment que les membres de la Commission nationale doivent prêter entre les mains de leur président. Le serment des agents de la Commission nationale est visé au paragraphe 3 de l'article 38.

Le Conseil d'Etat estime qu'en accord avec l'article 110 de la Constitution, le projet de loi sous revue est à compléter à l'effet d'imposer également au président la prestation d'un serment, d'en déterminer la formule et l'autorité appelée à le recevoir.

Article 37

Le paragraphe 1er précise que la Commission nationale est un organe collégial chargé d'établir son propre règlement intérieur appelé à en régir le fonctionnement. Ce règlement doit être publié au Mémorial.

Dans ce contexte, le Conseil d'Etat propose de ne pas mentionner le Mémorial „B", mais d'évoquer tout court le „Mémorial". Le paragraphe en cause est à adapter en conséquence.

Sous le paragraphe 2, la matière visée sous la lettre c) est à supprimer pour être en contradiction avec l'article 36 prévoyant que le président et le vice-président sont désignés par le Grand-Duc qui ne saurait être lié dans ce contexte par des modalités de désignation inscrites dans le règlement intérieur de la Commission nationale.

La Commission nationale est un organe collégial. Le paragraphe 1er prend soin de le souligner. Par ailleurs il faut se rappeler qu'elle est réduite à trois membres effectifs et trois membres suppléants, conformément à l'article 36, paragraphe 2. Le Conseil d'Etat en dégage un certain nombre de conclusions.

Il estime d'abord que ladite commission doit toujours siéger à trois, qu'elle doit systématiquement comprendre au moins un juriste et un informaticien et que les abstentions ne sont pas recevables. Il préconise en outre une solution alternative en matière de conflit d'intérêts dans le chef d'un membre. Le Conseil d'Etat compte de la sorte renforcer la cohérence et la collégialité de l'organe en cause, responsabiliser davantage les différents membres et tirer un maximum de profit de leurs compétences professionnelles respectives.

A cet effet, les paragraphes 3 à 6 se liront comme suit:

„(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. Elle 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."

Au paragraphe 7, compte tenu de la proposition de texte ci-dessus, le bout de phrase „pris à la majorité des membres présents" peut être supprimé.

Au paragraphe 8 se trouve confirmée et renforcée la disposition proposée par le Conseil d'Etat dans le cadre de l'article 36, paragraphe 1er, alinéa final.

Article 38

Cet article a pour principal objet de régir le statut des membres et agents de la Commission nationale.

Le paragraphe 2 prévoit d'abord que les membres et agents sont des employés privés assimilés aux employés de l'Etat. Ils sont donc soumis à la loi modifiée du 27 janvier 1972 fixant le régime de ces employés. Le même paragraphe 2 continue ensuite à préciser que cette assimilation s'effectue „sans préjudice des dispositions de la présente loi et de celles d'un règlement grand-ducal à prendre en matière de cadre, de rémunération et de promotion des *agents* de la Commission". Les membres de la Commission ne semblent donc pas être visés par cette réserve. Le commentaire de l'article est muet et quant à cette particularité et quant à la portée même de cette réserve.

Le paragraphe 3 règle le serment des agents, l'article 36, paragraphe 6 celui des membres de la commission nationale. Le Conseil d'Etat rappelle que le projet de loi sous revue ne comporte aucune prescription similaire pour le président de la Commission nationale et renvoie à ce propos à ses observations sous l'article 36, paragraphe 6 ci-avant.

Au paragraphe 6, il est prévu que „la Commission peut également faire appel à des experts externes qui sont *engagés* sur base d'un contrat de droit privé". Lue dans le contexte bien circonscrit de l'article 38, la disposition précitée prête à confusion alors que l'on pourrait en conclure que des experts externes pourraient en permanence être au service de la commission. Cette interprétation paraît encore être confortée par l'emploi du terme „engagés" qui laisse en effet entendre que ces experts s'ajoutent au personnel visé aux paragraphes 2 et 5.

Or le commentaire de l'article traduit une toute autre idée en expliquant que „la Commission doit avoir une certaine flexibilité et doit recourir *dans certains cas* (ex. traitement de données relevant du domaine scientifique tel que le génie génétique etc.) à des experts externes". Dans cette optique, le Conseil d'Etat propose de libeller en ces termes le paragraphe 6 de l'article 38:

„(6) 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."

Article 39

Au paragraphe 1er, il y a lieu de remplacer les termes impropres de „à faire part" par ceux de „*à charge*" du budget de l'Etat.

Il convient en outre d'écrire „L'Etat met à sa disposition les biens mobiliers et immobiliers nécessaires au bon fonctionnement et à l'exercice de ses missions" au lieu de „ainsi que d'un apport de biens …".

Au paragraphe 3, il est proposé d'écrire dans les deux phrases que la Commission nationale „*arrête* " plutôt qu'„approuve" son bilan, son rapport de gestion et son budget. Le Conseil d'Etat se demande en outre s'il n'est pas préférable de parler dans ce contexte d'un compte d'exploitation au lieu du „bilan" de l'exercice précédent qui serait à arrêter par l'organe en cause.

Au paragraphe 4, le Conseil d'Etat suggère de substituer aux mots „à faire part du" les termes „*à inscrire au*" budget de l'Etat.

Article 40

Conformément à l'article 12, paragraphe 2 du projet de loi sous examen, le responsable du traitement est exempté de l'obligation de notifier à la Commission nationale la mise en œuvre d'un traitement lorsqu'il a désigné „un chargé de la protection des données tenu notamment d'assurer, de manière indépendante, l'application des dispositions légales en la matière et d'établir un registre des traitements effectués par le responsable du traitement".

L'article 40 concerne plus particulièrement ce chargé de la protection des données.

Le paragraphe 2 détermine ses missions qui consistent à:

„a) assurer l'application des dispositions de la présente loi et de ses règlements d'exécution aux traitements qu'il est appelé à surveiller;

b) tenir un registre des traitements effectués par le responsable du traitement identique à celui tenu par la Commission quant à son contenu et son fonctionnement afin de garantir que ces traitements ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées."

De l'avis du Conseil d'Etat, il y a lieu de maintenir un certain parallélisme entre les deux dispositions susévoquées.[1] Aussi propose-t-il d'opérer par simple renvoi en complétant comme suit le paragraphe 1er de l'article 40:

„(1) Tout responsable de traitement peut, dans le cadre de l'article 12, paragraphe (2) (a) *et aux fins y visées*, désigner un chargé de la protection des données, dont il communique l'identité à la Commission *nationale*."

La cohérence de la démarche s'en trouve ainsi garantie et le paragraphe 2 de l'article 40 peut être abandonné comme étant devenu superflu.

Dans le cadre du paragraphe 4, il est proposé de remplacer les termes „et/ou" par „ou".

Au regard du paragraphe 6, un léger doute peut surgir au sujet de la définition des personnes pouvant „de plein droit" exercer l'activité de chargé de la protection. Le paragraphe 8 énumère les avocats, réviseurs d'entreprises, experts-comptables et médecins comme „professions réglementées" admises à exercer „immédiatement" l'activité susmentionnée. Dans les deux textes précités, ce sont probablement les mêmes qui sont visés. Dans le but d'éliminer toute équivoque en la matière, le Conseil d'Etat propose de remplacer au paragraphe 6 les termes „ou celles pouvant exercer cette activité de plein droit" par ceux de „*ou celles exerçant une des professions réglementées visées au paragraphe (8)*".

Le paragraphe 7 circonscrit le cercle des formations pouvant justifier l'agrément de personnes non admises de plein droit à l'exercice de l'activité en cause. Est visée, entre autre, la formation universitaire accomplie en „sciences de la nature" dont les contours sont quelque peu flous[2] et mériteraient d'être précisés. Pour pouvoir être agréés, les candidats doivent, en sus de la qualification requise, justifier d'„assises financières" d'une valeur de quinze millions de francs au moins, ce qui n'est pas négligeable. Contrairement à ce que laisse entendre le commentaire, une telle garantie de solvabilité ou de crédit n'est pas exigée par la loi du 31 mai 1999 régissant la domiciliation des sociétés à laquelle il est fait référence.

Elle paraît en outre disproportionnée par rapport aux obligations qu'elle est censée couvrir. Aussi convient-il de la réduire en conséquence, sinon même de l'abandonner carrément.

Selon le paragraphe 9, „la Commission vérifie les qualités de tout chargé de la protection des données qu'il soit agréé ou membre d'une des professions réglementées visées au paragraphe qui précède …". Le Conseil d'Etat met en question la nécessité d'examiner dans le chef d'une personne active dans le cadre d'une des professions réglementées énumérées au paragraphe 8 „son activité professionnelle antérieure à la désignation" et de la soumettre à un contrôle[3] de ses connaissances.[4] N'est-il pas suffisant de

1 Articles 12, paragraphe 2 et 40, paragraphe 2

2 L'astrologie, l'astronomie … sont-elles des sciences de la nature au sens du projet?

3 Même continu

4 A noter que la Commission nationale ne se voit pas attribuer positivement la compétence de vérifier la garantie financière prescrite?!

lui appliquer les sujétions découlant des pouvoirs d'opposition de la Commission nationale en vertu de l'alinéa 2 du paragraphe 9 de l'article 40 sous revue? En cas de réponse affirmative à cette interrogation, il faudrait adapter l'alinéa 1 en conséquence.

A l'alinéa 1 du paragraphe 9, il convient de substituer le terme „ou" aux signes „et/ou".

Article 41

Cet article institue un accès spécifique aux données concernant les abonnés aux services de télécommunications. Elle assimile dans ce contexte „toute personne agissant dans le cadre de la sauvegarde de la vie humaine" aux autorités compétentes visées aux articles 88-1 à 88-4 du code d'instruction criminelle et au procureur d'Etat agissant dans le contexte d'un flagrant délit. Cet accès a lieu de plein droit, mais sur requête et par l'intermédiaire de l'Institut luxembourgeois de régulation (IRL).

Dans sa teneur actuelle, l'article 41 du projet de loi est inacceptable.

En mettant sur un pied d'égalité les différents acteurs susmentionnés, obéissant chacun à des contraintes et intérêts spécifiques, le texte en question rend fastidieuse la recherche d'une solution à tous égards satisfaisante pour l'ensemble des situations visées. En outre, son articulation harmonieuse avec les dispositions de la directive 95/46/CE à transposer, mais aussi avec celles de la directive 97/66/CE du Parlement Européen et du Conseil du 15 décembre 1987 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications[1], est loin d'être établie, encore qu'il faille reconnaître que cette tâche n'est pas aisée. A première vue, les champs d'application respectifs des deux directives sont distincts, la directive 95/46 s'appliquant aux services de télécommunications qui ne sont pas accessibles au public à l'opposé de la directive 97/66 visant les services de télécommunications précisément accessibles au public. A y regarder de plus près, les choses se compliquent cependant considérablement.

Pour s'en convaincre, il suffit de se reporter aux considérants de la directive 97/66/CE et de relire l'article 14 du même instrument communautaire prévoyant expressément „l'extension du champ d'application de certaines dispositions de la directive 95/46/CE".

Dans les conditions données, le Conseil d'Etat recommande de procéder avec circonspection. Aussi est-il favorable à une approche par étapes.

Il propose ainsi de limiter dans une première phase la portée de l'article 41 aux demandes d'accès provenant des autorités compétentes visées aux articles 88-1 à 88-4 du code d'instruction criminelle et, en cas de flagrant délit, au procureur d'Etat.

L'extension ultérieure de cette mesure à „toute personne agissant dans le cadre de la sauvegarde de la vie humaine" mérite réflexion, afin d'éviter des demandes abusives et l'institution d'une procédure onéreuse et disproportionnée par rapport aux intérêts réels en jeu. Pour l'instant, il ne semble pas y avoir péril en la demeure, les services de secours ne paraissant pas en l'état actuel de la situation de fait et de droit être outre mesure entravés dans les actions qu'ils mènent dans l'intérêt de la sauvegarde de la vie humaine.

Par déduction des développements qui précèdent, il y a donc lieu de remanier en conséquence l'article 41 du projet de loi sous examen qui s'énoncera comme suit:

„**Art. 41. –** ***Dispositions spécifiques***

(1) Les autorités compétentes visées aux articles 88-1 à 88-4 du code d'instruction criminelle et le procureur d'Etat agissant en matière de flagrant crime accèdent de plein droit, sur requête et par l'intermédiaire de l'Institut luxembourgeois de régulation (ILR) aux données concernant les abonnés des opérateurs de télécommunications, des services postaux et des fournisseurs de ces services. A ces fins, les opérateurs et les fournisseurs mettent d'office et gratuitement à la disposition de l'ILR les données relatives aux abonnés et leurs services. Les données doivent être mises à jour 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 télécommunications 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 mises à disposition des données.]

1 Publiée au J.O.C.E. No L24 du 30.1.1998

(2) 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 ainsi que celles prises en matière de flagrant crime.

(3) L'ILR peut entièrement automatiser cette procédure suite à l'autorisation de la Commission nationale. La Commission nationale vérifiera en particulier la sécurisation du système informatique utilisé."

Les modifications autres que celles dictées par les considérations qui précèdent sont motivées comme suit:

– Aux deux premiers paragraphes, la notion de „flagrant délit", tirée du langage courant, a été remplacée par celle de „flagrant crime" à connotation juridique bien plus précise.
– Les deux premières phrases du paragraphe 1er font l'objet de quelques amendements rédactionnels n'altérant en rien la portée du projet.
– Quant à la phrase finale du même paragraphe, il y a lieu de s'interroger sur la nécessité de prévoir un règlement grand-ducal afin de déterminer les services, opérateurs et fournisseurs pressentis pour collaborer avec l'ILR. Tous les acteurs de l'espèce actifs sur le territoire national ne sont-ils pas d'office censés devoir agir de la sorte? En ordre subsidiaire, il est superfétatoire de préciser que l'obligation pour ces acteurs d'ouvrir à l'ILR l'accès aux données concernant leurs abonnés se situe „dans le cadre de l'article 41 paragraphe (1)".
– L'utilité du maintien, dans le nouveau contexte, du paragraphe 3 n'est plus donnée. L'on doit en effet raisonnablement pouvoir admettre que l'ILR s'exécute immédiatement lorsqu'elle est sollicitée par les autorités visées au paragraphe 1er ou encore en matière de flagrant crime. Aussi la disposition du paragraphe 3 a-t-elle été omise dans la version proposée par le Conseil d'Etat.
– Le paragraphe 4 (3 selon le Conseil d'Etat) prévoyant que l'ILR peut automatiser la procédure applicable précise de façon superflue que „cette automatisation permettra l'accès par voie électronique et sans qu'une intervention manuelle soit requise". N'est-ce pas en effet l'essence même d'une automatisation?
– Dans la nouvelle constellation, le dernier paragraphe a dû être abandonné, car les informations recueillies à des fins de poursuite pénale doivent par définition pouvoir faire l'objet d'un traitement ultérieur.

Article 42

Le Conseil d'Etat propose de compléter cet article par un paragraphe (4) nouveau libellé comme suit:

„(4) Les articles 12-1 et 28-1 de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques continueront à servir de fondement juridique aux règlements d'application afférents."

Cet ajout a pour objet de garantir la validité des règlements grand-ducaux concernant les banques de données pénales et médicales. Sont plus précisément visés:

– le règlement grand-ducal du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale, pris sur la base de l'article 12-1 de la loi précitée de 1979;
– le règlement grand-ducal du 2 octobre 1992 réglementant l'utilisation des données nominatives médicales dans les traitements informatiques;
– le règlement grand-ducal du 9 août 1993 autorisant la création et l'exploitation d'une banque de données nominatives constituant la partie nationale du système d'information Schengen (N.SIS).[1]

Article 43

Sans observation.

1 dont la base légale est d'ailleurs constituée – en dehors de la loi du 31 mars 1979 – par la loi du 3 juillet 1992 (Accord de Schengen)

Article 44

Cette disposition finale[1] doit prendre, compte tenu de la proposition de texte du Conseil d'Etat au regard de l'article 42 ci-dessus, la teneur suivante:

„**Art. 44.–** *La loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques est abrogée, sous réserve de la mesure transitoire inscrite au paragraphe (4) de l'article 42.*"

Il ne se recommande pas de mentionner dans ce contexte les différentes lois modificatives de l'instrument de base.

Quant aux règlements grand-ducaux, il faut d'abord rappeler qu'ils ne sauraient être ni maintenus ni abrogés par la loi, et ce par application des principes tirés de la hiérarchie des normes et du parallélisme des formes. Abstraction faite de cette observation formelle, le Conseil d'Etat se demande toutefois s'il ne s'impose pas de précisément maintenir en vigueur un certain nombre de règlements grand-ducaux édictés sur la base de la loi du 31 mars 1979.

A cet effet, le Conseil d'Etat a prévu sous l'article 42, paragraphe 4, le maintien provisoire des articles 12-1 et 28-1 de la loi de 1979.

Le pouvoir réglementaire doit, quant à lui, veiller à abroger les règlements grand-ducaux n'ayant plus leur place dans le nouveau cadre légal que tend à instituer le projet de loi sous avis.

Article 45

Le Conseil d'Etat se demande s'il est raisonnable de prévoir l'entrée en vigueur du texte sous revue pour le premier jour du mois qui suit la publication au Mémorial. Ne serait-il pas plus réaliste, compte tenu des implications incisives de la loi à intervenir, de ménager la transition et de prévoir un délai de quelques mois entre sa publication et sa date d'effet?

Ainsi délibéré en séance plénière, le 29 janvier 2002.

Le Secrétaire général, — *Le Président,*

Marc BESCH — Marcel SAUBER

1 Il ne convient pas, dans ce contexte, de parler de dispositions finales

4735/09

N° 4735[9]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

AVIS DE LA CHAMBRE DE COMMERCE

DEPECHE DU MINISTRE AUX RELATIONS AVEC LE PARLEMENT AU PRESIDENT DE LA CHAMBRE DES DEPUTES

(19.6.2002)

Monsieur le Président,

A la demande du Ministre délégué aux Communications, j'ai l'honneur de vous faire parvenir en annexe *l'avis de la Chambre de Commerce* sur le projet de loi sous rubrique.

Veuillez agréer, Monsieur le Président, l'assurance de ma haute considération.

Pour le Ministre aux Relations avec le Parlement,
Daniel ANDRICH
Conseiller de Gouvernement 1re classe

*

AVIS DE LA CHAMBRE DE COMMERCE

(13.2.2002)

Par sa lettre du 15 décembre 2000, Monsieur le Ministre délégué aux Communications a bien voulu saisir la Chambre de Commerce pour avis du projet de loi sous rubrique.

Le présent projet de loi a pour objet de transposer la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et est amené à remplacer l'actuelle loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, telle que modifiée. Il est à noter que les Etats membres avaient jusqu'au 24 octobre 1998 pour transposer ladite directive. Le Luxembourg a été condamné par la Cour de Justice des Communautés Européennes par un arrêt du 4 octobre 2001, suite à un recours en manquement introduit en décembre 2000. Il y a donc urgence à adopter une nouvelle loi en matière de protection des données, non seulement pour se conformer au droit communautaire, mais également du fait que la loi du 31 mars 1979 est devenue largement obsolète.

1. Considérations générales et introductives

Le développement de l'économie numérique va de pair avec une croissance des mouvements et échanges internationaux de données de toutes sortes, dont notamment les données à caractère personnel. Standards ouverts et le caractère global des réseaux permettent et facilitent la transmission des données en les mettant ainsi à la disposition de tout le monde. Il y a aujourd'hui un consensus général à considé-

rer que la croissance et le développement de la société de l'information, et avec elle du commerce électronique, est largement tributaire du niveau de protection réservé aux données en circulation. Une réglementation au niveau mondial s'impose dès lors au vu de la mondialisation des réseaux et de la libre circulation des données.

Alors que la protection des données à caractère personnel faisait traditionnellement l'objet d'une réglementation juridique afin de protéger la sphère de l'intimité de l'individu, les données à caractère personnel ont aujourd'hui tendance à être considérées comme étant une marchandise et revêtant une certaine valeur marchande. Cette tendance est nettement plus exprimée de l'autre côté de l'Atlantique et s'imposera au fur et à mesure de la mondialisation des échanges commerciaux par les réseaux. Dès lors, toute réglementation en la matière constituera nécessairement une tentative de conciliation entre le respect des droits et libertés fondamentaux des individus d'une part, et les intérêts commerciaux internationaux d'autre part.

A première vue, la directive 95/46/CE, et avec elle le projet de loi No 4735, semblent ainsi être en opposition à l'atmosphère générale du monde développé qui tend vers plus de transparence, d'ouverture et de communication et où s'établit une culture du tout-connaître, voire du tout-publier.

Ce climat de transparence est très largement influencé par la mentalité anglo-saxonne qui se veut plus ouverte et qui considère que celui qui n'a rien à se reprocher n'a rien non plus à cacher. Les moyens informatiques modernes ont donné aux adeptes de la transparence les moyens techniques de leur ambition. Que ce soient les Etats, que ce soient les médias, que ce soit le monde commercial, tous entendent profiter de ce climat de transparence pour y établir leurs intérêts de pouvoir et d'argent. A cet égard, le secteur financier luxembourgeois, par exemple, est bien placé pour constater que le droit fondamental à la discrétion et au secret est attaqué de toutes parts. Le droit au secret, le droit à l'intimité privée, le droit de se taire sont des droits qui s'apprêtent à céder le pas.

Dans la discussion publique des objectifs contradictoires se distinguent:

➢ la transparence serait une vertu en soi; l'individu aurait à céder devant une multitude de causes, comme:
  - la liberté de la presse dans un univers médiatisé à l'extrême, le droit à l'information, le droit d'être informé,
  - la lutte contre le crime international et organisé, plus généralement, la sécurité des hommes et des biens qui appelle une internationalisation de la justice et des moyens d'enquête,
  - l'égalité du citoyen devant l'impôt,
  - la gestion informatique du service public,
  - plus généralement le traitement de masse de tous les bienfaits d'une société de consommation.

➢ Parallèlement, la protection de la vie privée et des droits de l'homme en général, la protection des données nominatives ou encore la protection des droits de l'individu en face d'une administration toute-puissante sont des sujets d'actualité. Il est admis qu'un Etat de droit digne de ce qualificatif doit une protection renforcée à l'individu devant la curiosité publique. La directive prétend répondre à cette aspiration.

Dans le souci de bien faire, les législateurs européens ont une nette tendance à prendre résolument les deux directions à la fois. De plus en plus, le monde politique demande de la transparence; de plus en plus aussi il tente également de protéger l'individu. Cette contradiction peut se retrouver parfois dans un seul et même texte de loi. Le secteur financier en constitue un exemple flagrant:

- Les données secrètes des clients de banques sont accessibles aux autorités de contrôle ou à d'autres organismes investis d'une mission publique, mais ceux-ci sont alors soumis à un même secret. Ces autorités peuvent quelquefois partager les données recueillies avec leurs homologues étrangers, là encore sous la condition que ceux-ci soient soumis à un secret équivalent, et ainsi de suite. En fin de compte, on se demande si on n'aboutit pas dans un système où tout le monde a le droit de tout savoir à condition de le tenir secret.
- On demande aux banques d'indiquer à chaque paiement toutes les données permettant une identification des donneurs d'ordres et des bénéficiaires concernés. La Commission européenne de son côté veut imposer aux banques une protection accrue de ses mêmes données tout en exigeant par ailleurs une accélération des paiements des virements transfrontaliers.

- L'Europe s'apprête à collecter les données sur les intérêts de l'épargne de centaines de millions de citoyens, à les traiter par ordinateur, à les envoyer vers d'autres ordinateurs, pour contrôler, enquêter, interconnecter.

Les défenseurs d'une idée de protection de la vie privée et aussi de protection du traitement des données nominatives semblent bien perdus dans ce climat. Par la directive 95/46/CE, les décideurs politiques européens ont voulu donner l'impression d'attacher encore une importance à cette idée. Ils ne sont cependant pas crédibles dans leur démarche alors qu'ils font tout par ailleurs pour organiser la transmission de données au-delà des frontières et au-delà des organisations. Ainsi, la directive apparaît comme l'alibi politique en face d'un droit qui disparaît, et non pas comme une tentative d'endiguer la tendance. Que ceux qui voudraient croire que la future législation sur le traitement des données va donner au citoyen des garanties se détrompent. Elle va au contraire rendre impossible d'opposer aux autorités des Etats qui réclament des données toutes considérations de protection fondées sur le droit national.

En cas de doute, la crainte diffuse devant ces orientations est combattue par les Etats avec une nette tendance des Etats à se faire confiance tout en se méfiant des opérateurs privés et commerciaux. Le même phénomène se manifeste dans le projet de loi sous avis qui admet des exceptions, p. ex. au droit à l'information des personnes concernées, en faveur de la poursuite des infractions, de la sûreté de l'Etat, de la défense et de la sécurité publique. En d'autres termes, l'Etat se considère au-dessus des soupçons qui lui semblent néanmoins justifiés vis-à-vis des entreprises. Si le texte prend garde de ne jamais s'appliquer lorsque les domaines sensibles de l'Etat et donc les libertés publiques sont concernés, il établit par contre une foule de chicanes pour les organisations privées. Une charge administrative considérable attend les entreprises dont on soupçonne l'abus permanent et systématique lorsqu'ils traitent les données personnelles dont ils disposent. Des peines pénales excessives viennent frapper ceux qui négligent la moindre des innombrables procédures prescrites. Si on doit comprendre la nécessité objective des traitements de données par l'Etat dans certains domaines sensibles, on doit tout de même regretter que ce pragmatisme fasse défaut par ailleurs. Ceci d'autant plus que le danger informatique, s'il existe, ne vient pas des opérateurs privés. Ils sont certes en mesure de causer un dommage par l'utilisation et la propagation de données fausses ou simplement privées, ils ne représentent pas pour autant une menace pour les libertés publiques.

Il serait illusoire de penser que le Luxembourg puisse renverser les tendances à cet égard. Les commentaires de la Chambre de Commerce qui suivent se veulent dès lors de rester constructifs dans une matière qui est largement technique et qui est de toute façon dictée par le droit européen. Il convient cependant de ne pas se voiler la face sur la direction que prennent les choses et de rappeler que cette loi se lira plus utilement en gardant à l'esprit les domaines de la vie privée qui s'effritent et que ce texte ne peut ni ne veut protéger.

2. Une transposition tardive et incomplète des directives communautaires

Il est à noter que la directive 97/66/CE du 15 décembre 1997, qui est venue compléter les dispositions de la directive 95/46/CE en ce qui concerne plus particulièrement le secteur des télécommunications, aurait dû être transposée avant le 24 octobre 1998. Le présent projet de loi aurait pu être l'occasion de transposer les deux directives communautaires. Par ailleurs, le contenu de la proposition de directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques aurait de même pu être pris en considération dans la mesure où ce texte reprend les dispositions de la directive 97/66/CE en les appliquant au secteur des communications électroniques.

Alors que le Luxembourg entend se présenter comme une plate-forme internationale en matière de commerce électronique et s'est doté à cette fin d'une loi-cadre en ce domaine, aucune disposition du projet de loi ne vise spécifiquement la protection des données personnelles dans le cadre de l'utilisation de techniques de communications électroniques. Il est à noter à cet égard que l'avant-projet de loi sur le commerce électronique comportait un chapitre spécifique à la protection des données personnelles qui visait notamment à transposer certaines dispositions de la directive 97/66/CE en droit luxembourgeois dans ses aspects liés au commerce électronique. La Chambre de Commerce a dû assister au démantèlement de cet avant-projet de loi et en particulier au retrait du chapitre relatif à la protection des données. Pourtant, les auteurs de ce projet de loi se proposaient de traiter cette partie du texte dans la future loi relative à la protection des données personnelles. Il s'avère toutefois qu'il n'en est rien. Le Conseil

d'Etat, dans son avis du 2 mai 2000 (Doc. parl. No 4641[1], pp. 2-3), avait néanmoins insisté pour que les lacunes de la loi relative au commerce électronique soient comblées le plus rapidement possible. Il est à souligner que les violations de la vie privée sont la crainte majeure des utilisateurs d'Internet et que cette crainte constitue un important obstacle au développement du commerce électronique. Bien que l'exposé des motifs précise que le projet de loi vient compléter la loi sur le commerce électronique et ainsi parfaire le „*dispositif de sécurisation juridique*" du commerce électronique, le présent texte ne contient aucune disposition relative à la confidentialité des communications ou aux obligations des fournisseurs de service de communication électronique lors de la transmission de données. Il est précisé dans l'exposé des motifs (Doc. parl. No 4735, p. 86) que ces aspects essentiels en matière de commerce électronique devront faire l'objet d'un règlement grand-ducal. La Chambre de Commerce estime que des dispositions aussi fondamentales auraient leur place dans une loi plutôt que dans un règlement grand-ducal et que la loi adéquate reste celle relative au commerce électronique.

3. Un champ d'application imprécis

Il est indéniable que l'évolution de l'utilisation des ordinateurs dans les années 90 n'était en rien prévue lors de la rédaction de la loi de 1979. Les dispositions de cette loi sont aujourd'hui devenues difficilement applicables et largement inappliquées. Le décalage actuel de la loi de 1979 par rapport à la réalité est à garder en mémoire afin d'éviter, dans un nouveau texte, de renouveler les mêmes erreurs. Or le projet, du fait de son champ d'application extrêmement large qui tend à couvrir toutes les situations de traitement possibles, risque d'être tout aussi difficilement applicable que le texte actuel. De plus, il semble aux yeux de la Chambre de Commerce qu'un certain nombre de dispositions soit difficilement compatible avec certaines activités du secteur financier notamment.

3.1. *Des définitions trop extensives*

Le champ d'application du projet de loi est déterminé en son article 3, qui est repris de l'article 3 de la directive communautaire. Ce dernier est à lire en relation avec l'exposé des motifs de la directive qui précise que les traitements portant sur des données relatives aux personnes physiques ne sont couverts par la directive „*que s'ils sont automatisés ou si les données sur lesquels ils portent sont contenues dans un fichier structuré selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause*". Même si le traitement manuel des données personnelles y est visé, il est précisé que „*les dossiers ou ensembles de dossiers qui ne sont pas structurés selon des critères déterminés n'entrent en aucun cas dans le champ d'application*" de la directive. Cette précision est à mettre en rapport avec le champ d'application du projet de loi tel qu'il ressort des définitions qui figurent à l'article 2. Si la définition du concept de „*traitement de données à caractère personnel*" est strictement repris de la directive 95/46/CE, il n'en est pas de même de la notion de „*fichier de données à caractère personnel*" qui est défini comme „*tout ensemble structuré ou non de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique*". Une telle définition tend notamment à s'appliquer à tout dossier ouvert et tenu par une entreprise en contact avec son client. Il en est de même pour les dossiers ouverts pour chaque salarié et tenus dans les départements des ressources humaines et services de personnel des entreprises. Il serait en effet inconcevable qu'un salarié ait accès par exemple à des notes confidentielles contenues dans son dossier, et encore moins qu'il ait un droit de rectification concernant de telles notes. Le caractère excessif de cet écart par rapport à la directive vient surtout du fait que le champ d'application du texte dépasse les applications purement informatiques, contrairement à la loi luxembourgeoise actuelle.

La combinaison de la définition de la notion de „*fichier*" avec l'obligation d'autorisation préalable pour ce qui est du traitement concernant le crédit et la solvabilité des personnes concernées, visé à l'article 14 du projet de loi, conduit à ce que l'une des activités principales du banquier soit soumise à l'autorisation préalable de la Commission Nationale pour la Protection des Données. Cela ne peut pas être la volonté du législateur. Il est permis d'ajouter à ce sujet qu'une telle autorisation préalable, s'appliquant aux établissements de crédit, est incompatible avec le principe, énoncé tant dans la directive 95/46/CE qu'à l'article 5 du projet de loi, selon lequel le traitement de données à caractère personnel est légitime, en particulier lorsqu'il est nécessaire à la conclusion ou à l'exécution d'un contrat liant la personne concernée. Or la légitimité, précise l'exposé des motifs du projet de loi, „*est ce qui fonde un*

responsable de traitement à agir en tant que tel". Dès lors que le traitement est légitime, aucune autorisation préalable ne devrait en toute logique être requise.

En conséquence, la Chambre de Commerce demande instamment à ce que, d'une part, la définition du terme „*fichier*" ne couvre que les „*ensembles structurés de données*" et que soient donc supprimés les mots „*ou non*" de cette définition, de telle sorte que la constitution de simples dossiers soit exclue du champ d'application du texte, conformément à la directive 95/46/CE, et que, d'autre part, l'obligation d'autorisation préalable pour ce qui est du traitement concernant le crédit et la solvabilité des personnes concernées, visé à l'article 14 du projet de loi, ne concerne que les personnes dont le métier n'est pas d'octroyer des crédits.

Par ailleurs, le commentaire des articles parle de traitements concernant spécialement le crédit et la solvabilité, quelle que soit la profession en cause (banque, assurances ou autres professionnels du secteur financier). Selon les auteurs du projet de loi, de tels traitements conditionnent l'accès au contrat et devront donc être soumis à autorisation préalable.

En ce qui concerne les traitements en matière d'assurance, la Chambre de Commerce comprend mal quels traitements seraient visés (alors que l'assureur ne s'intéresse normalement pas au crédit et à la solvabilité des clients). La Chambre de Commerce demande par conséquent que la référence à l'assurance soit supprimée dans le commentaire afférent à l'article précité.

L'article 2 (a) définit les données à caractère personnel comme étant „*toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable (…)*". Toutefois, la notion de données à caractère personnel telle que définie dans la directive ne comprend ni le son, ni les images comme information concernant une personne. Il en va de même des dispositions concernant la surveillance, définie à l'article 2 (h) et réglementée à l'article 10 du projet de loi sous rubrique. La directive n'entend nullement régler l'activité de surveillance. La Chambre de Commerce est d'avis qu'une telle réglementation n'a pas non plus sa place dans un projet de loi destiné à constituer un cadre légal pour l'utilisation des données à caractère personnel.

Pour autant que le projet de loi sous analyse devrait continuer à régir ces activités de surveillance, la Chambre de Commerce voudrait remarquer qu'elle s'oppose à ce qu'un traitement à des fins de surveillance sur le lieu de travail, tel que prévu à l'article 11 du projet de loi, soit soumis à une autorisation préalable de la Commission (article 14 (1) du projet de loi) et que cette autorisation soit subordonnée à l'avis préalable de l'Inspection du Travail et des Mines (article 14 (2) du projet de loi). On tente ici de réintroduire en catimini le système de l'autorisation préalable, système qui a pourtant fait la preuve de ses faiblesses. La Chambre de Commerce est en effet d'avis qu'une telle surveillance, plutôt que de restreindre un prétendu droit à la vie privée sur le lieu de travail, permet aux entreprises d'honorer pleinement les obligations qui leur incombent sur base de la législation sur la sécurité et la santé au lieu de travail et ceci surtout lorsqu'il s'agit de postes de travail individuels et à haut risque. Il s'y ajoute que, compte tenu du fait de la propagation des nouvelles technologies de l'information et de la communication au sein des entreprises et de leur usage facile, la tentation d'utiliser ces technologies à des fins privées est un risque réel pour l'entreprise. La submersion du poste de travail du salarié par un flot de courriers électroniques privés se traduit évidemment par une perte de la capacité de stockage du matériel informatique qui est d'autant plus importante que les courriers en question contiennent souvent des annexes exubérantes en *bits* et, en conséquence, gourmandes d'espace de mémoire. Toutefois, et c'est là le problème majeur, la consultation des courriers électroniques reçus et l'envoi de tels courriers par le salarié prend un certain temps qui va évidemment au dépens de l'employeur, alors qu'il s'agit de temps de travail rémunéré. Finalement, il ne faut pas oublier que l'envoi de courrier électronique génère des coûts téléphoniques. La Chambre de Commerce est dès lors d'avis qu'il convient de mettre les employeurs en mesure de recourir à des techniques de surveillance, sans qu'ils aient besoin pour cela d'avoir l'accord préalable du salarié, ni d'une quelconque autre instance ou autorité. Aux yeux de la Chambre de Commerce, une simple information à cet égard à l'adresse du salarié devrait suffire.

3.2. *Des situations ambiguës*

L'article 11 prévoit la surveillance sur le lieu de travail. Aux termes dudit article un tel contrôle n'est autorisé que s'il est temporaire (article 11 point 1 du projet de loi). A cet égard, la Chambre de Commerce s'interroge si cette condition est compatible avec le contrôle effectué dans le cadre d'un système d'horaire mobile.

4. La spécificité de certains types de données

4.1. *La spécificité de certaines informations traitées par les banques*

La Chambre de Commerce souhaite attirer l'attention des auteurs du projet de loi sur la spécificité de certaines informations traitées par les banques. Dans le cadre de la lutte contre le blanchiment, les banques sont tenues, en vertu de l'article 39 (2) et (4) de la loi du 5 avril 1993 sur le secteur financier, d'identifier non seulement leurs clients mais également les personnes avec lesquelles elles effectuent des transactions à titre occasionnel dès lors qu'il existe un soupçon de blanchiment. Les banques sont tenues de conserver les données relatives à ces personnes pendant une durée de cinq années à compter de l'exécution de la transaction. Quand bien même la banque se serait abstenue d'effectuer une transaction en raison de soupçons de blanchiment, il est plus qu'opportun qu'elle retienne les données relatives à ces personnes sans que celles-ci soient obligatoirement informées du traitement dont elles font l'objet.

Une logique similaire opère au regard de la lutte contre la corruption et le détournement de fonds publics, au titre de laquelle la Commission de surveillance du secteur financier, dans sa circulaire No 2000/21, impose aux banques *„d'instaurer des procédures de contrôle particulières, afin de s'entourer de toutes les garanties nécessaires*" dans leurs relations *„avec des personnes exerçant des fonctions publiques importantes dans un Etat ou des personnes et sociétés qui, de manière reconnaissable, leur sont proches ou leur sont liées*". Il est parfaitement légitime, sinon légalement requis, que les banques constituent, pour ce faire, des fichiers de personnes à risque, voire indésirables. Ces fichiers peuvent aussi bien contenir les noms de personnes avec lesquelles la banque a pu être en contact que ceux de personnes avec lesquelles elle ne souhaite pas ou n'est pas en droit d'établir de relations. Il peut par exemple s'agir des personnes à l'encontre desquelles il existe des mesures restrictives ou d'autres personnes faisant l'objet de sanctions au titre de la politique étrangère et de sécurité commune de l'Union européenne.

L'existence même de ces fichiers, indispensables au bon fonctionnement des établissements de crédit, ne doit pas être mise en péril par le droit, prévu à l'article 26 du projet de loi, des personnes concernées à être informées. Au regard de la lutte contre le blanchiment, y compris la corruption, la Chambre de Commerce considère que la collecte des données entre logiquement dans le champ d'application des exceptions au droit à l'information prévues à l'article 27 (1) du projet de loi sous examen, au titre de *„la prévention, la recherche, la constatation et la poursuite d'infractions pénales*".

4.2. *Les fichiers „fraude" dans le secteur des assurances*

Conformément aux dispositions de la Directive 95/46, l'article 5 du projet de loi prévoit différentes conditions, en application desquelles un traitement portant sur des données à caractère personnel est considéré comme légitime. Ces conditions viennent remplacer l'unique condition de licéité jadis retenue par la loi du 31 mars 1979, à savoir l'autorisation préalable de toute création et exploitation d'une banque de données.

La Chambre de Commerce est d'avis que la condition de licéité tenant à l'intérêt légitime devrait également pouvoir servir de base à la mise en place d'un fichier fraude. La lutte contre la fraude à l'assurance poursuit certainement un but légitime. La fraude a inévitablement des répercussions sur le niveau des primes d'assurance et pénalise ainsi la très grande majorité des assurés non fraudeurs.

La Chambre de Commerce rappelle à cet égard les inquiétudes du secteur des assurances au sujet des chiffres relatifs au phénomène de la fraude à l'assurance. Le Grand-Duché de Luxembourg est en retrait par rapport à ses voisins étrangers en ce qui concerne les moyens législatifs disponibles pour combattre de façon convenable ce problème.

En effet, la plupart de nos pays voisins (dont notamment la Belgique et l'Allemagne – pays pourtant bien connu pour ses susceptibilités en cette matière) ont mis en place des fichiers centraux performants, basés sur des informations nominatives, qui permettent de lutter efficacement contre le fléau de la fraude à l'assurance, coûtant en définitive très cher à la grande majorité des assurés.

Malheureusement, notre législation sur la protection des données nominatives ne permet pas, dans sa teneur actuelle, de recourir à de tels dispositifs informatiques. En l'absence d'adaptation de ladite législation, le secteur des assurances restera démuni face à la réalité de la fraude à l'assurance.

Il s'y ajoute que la fraude à l'assurance revêt une dimension de plus en plus internationale, notamment à travers le phénomène de la criminalité organisée sévissant dans plusieurs pays, ce qui rend indispensable une coopération internationale efficace à laquelle le secteur des assurances luxembourgeois doit malheureusement rester à l'écart du fait que le cadre légal ne permet pas la mise en place des applications informatiques appropriées.

4.3. *Le défaut d'exclusion concernant les données à caratère public*

Aux yeux de la Chambre de Commerce, le texte projeté comporte une lacune majeure dans la mesure où il omet de distinguer entre les données à caractère privé et celles à caractère public. Il est légitime que les premières soient protégées. En revanche, le caractère public des secondes devrait autoriser un traitement libre de celles-ci.

– Il peut s'agir de données manifestement publiques, telles que les informations connues de tous au sujet des personnalités célèbres. Ces données sont effectivement visées à l'article 6 (2) (e) du projet de loi qui prévoit une exception à l'interdiction du traitement de certaines catégories particulières de données.
– Il peut par ailleurs s'agir de données rendues publiques par la personne concernée elle-même. Ainsi les données figurant dans un annuaire téléphonique national devraient-elles légitimer la constitution de fichiers et la préparation de correspondance par les machines de traitement de texte.
– Il peut s'agir enfin des données rendues publiques par l'autorité publique. Il en est ainsi, à titre d'exemple, des listes de faillites ou des listes des établissements de crédit établies par la Commission de surveillance du secteur financier.

La Chambre de Commerce soutient vivement que de telles données publiques devraient être traitées différemment des données à caractère privé recueillies auprès de la personne concernée. Il est à noter à cet égard que la directive 95/46/CE vise uniquement la protection des données concernant les personnes physiques et n'impose donc aucune obligation relative au traitement des données concernant des personnes morales. Or, la protection des personnes morales par rapport aux traitements de données, prévue par le projet de loi, a pour corollaire un certain nombre d'obligations à charge des responsables de traitement. Ce sont précisément ces obligations qui sont en décalage par rapport au caractère public de certaines informations relatives aux personnes morales. C'est pour cette raison que la Chambre de Commerce plaide pour une exclusion des données publiques concernant des personnes morales du champ d'application du texte. Il est rendu attentif à cet égard à la définition très large du terme „*traitement*“ qui peut inclure des envois par télécopie ou l'utilisation de machines de traitement de texte.

4.4. *L'extension du champ d'application aux activités relevant de l'Etat*

Le champ d'application du texte s'étend également, selon les termes de l'article 3 (5) au traitement ayant pour objet la sécurité publique, la défense, les activités relatives à des domaines du droit pénal, la sûreté de l'Etat ou le bien-être économique de l'Etat lorsque celui-ci est lié à la sûreté de l'Etat. L'article 17 du projet de loi prévoit parallèlement que les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique feront l'objet d'un règlement grand-ducal.

Si donc les dispositions impératives du texte s'imposent aussi à l'Etat, il est à observer que les multiples limitations et dérogations prévues laissent douter de la volonté des auteurs de réellement soumettre les services de l'Etat à l'ensemble des obligations prévues. L'application aux administrations étatiques semble faite pour leur permettre de légitimer certaines actions et non pas pour leur imposer de nouvelles obligations. Cette réalité est flagrante en ce qui concerne les droits les plus importants dont bénéficient les personnes concernées par un traitement. Ainsi la sauvegarde de la sûreté de l'Etat, de la défense ou de la sécurité publique justifient-elles des dérogations aux obligations relatives au droit à l'information de la personne concernée (article 27 du projet de loi) et au droit d'accès aux données la concernant (article 29 du projet de loi). De plus, la sauvegarde d'un „*intérêt économique ou financier important de l'Etat, en particulier dans les domaines monétaire, budgétaire et fiscal*“ justifie l'absence de droit d'information des personnes concernées. Sur cette base, l'Etat pourrait ainsi refuser tout droit d'information aux administrés en ce qui concerne les données collectées à des fins d'imposition. La Chambre de Commerce considère qu'une telle prérogative est exorbitante. Elle l'est d'autant plus que l'harmonisation européenne du traitement des donneés va rendre impossible d'opposer des arguments de protection de la vie privée à la curiosité transfrontalière d'autres Etats européens.

5. Des sanctions disproportionnées et trop nombreuses

Le champ d'application extrêmement large du projet de loi est à mettre en relation avec les sanctions qui sont attachées à tout manquement aux obligations qui y figurent. La grande sévérité des peines apparaît comme disproportionnée par rapport aux faits incriminés. Ainsi, le fait d'avoir omis d'informer une personne après avoir, par exemple, relevé son numéro de téléphone et son adresse est punissable d'une peine d'emprisonnement de un an et d'une amende de 5.000.000 LUF. Une telle disproportion entre la gravité des actes et la lourdeur des peines encourues est d'autant plus contestable que le projet de loi ne prend aucunement en compte l'élément moral de l'infraction. Ainsi, celui qui a omis de se conformer à la loi par simple négligence sera punissable comme celui qui s'est sciemment soustrait aux obligations qui y sont imposées. La Chambre de Commerce réclame que les peines soient revues à la baisse et adaptées à la gravité des faits et que le mot „*sciemment*" soit ajouté à un certain nombre de dispositions d'ordre pénal qui figurent dans le projet de loi, en particulier aux articles 5 (2) et 26 (4). La Chambre de Commerce estime que, dans les hypothèses les moins graves, les sanctions administratives prévues à l'article 35 du projet de loi sous analyse sont suffisantes.

Dans ce contexte, la Chambre de Commerce voudrait également rendre attentif à l'article 23 (h) qui exige que les mesures relatives à la sécurité des traitements doivent „*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*". On impose ici au responsable du traitement une obligation qui est hors de son rayon de contrôle et d'influence, obligation qui est pourtant sanctionnée par une disposition pénale.

Par ailleurs, la Chambre de Commerce est d'avis que le nombre de sanctions pénales est démesuré et que leur dispersion devrait faire l'objet d'un regroupement dans un chapitre intitulé „Dispositions pénales".

Il est à remarquer que les montants devraient désormais être indiqués en euros et non plus en francs luxembourgeois.

6. L'interconnexion, un danger pour la vie privée

L'interconnexion est conçue par le projet de loi comme „*la corrélation de données traitées pour une finalité avec des données traitées pour une autre finalité par le même responsable du traitement ou par d'autres responsables de traitement*". La Chambre de Commerce se demande si le concept même „*d'interconnexion*" tel que défini dans le projet est compatible avec les droits des personnes concernées. La directive 95/46/CE précise que „*les finalités des traitements ultérieurs à la collecte ne peuvent pas être incompatibles avec les finalités telles que spécifiées à l'origine*". L'exposé des motifs du projet de loi précise certes que le principe de finalité est le principe fondateur du texte et „*qu'il ne serait pas opportun d'ouvrir, par le biais de l'interconnexion, une brèche dans ce principe fondamental*". Toutefois, à peine le principe de finalité réaffirmé, l'exposé des motifs s'empresse de l'écarter expressément puisqu'il est précisé que la notion d'interconnexion couvre „*la corrélation de données traitées pour une finalité avec des données traitées pour une autre finalité*". L'interconnexion ainsi définie apparaît quelque peu contraire aux principes énoncés par la directive. Il est à rappeler à cet égard que l'article 6 (1) de la directive impose aux Etats membres de prévoir que les données à caractère personnel soient „*collectées pour des finalités déterminées, explicites et légitimes*" et ne soient pas „*traitées ultérieurement de manière incompatible avec ces finalités*".

Si l'article 16 soumet l'interconnexion à l'autorisation préalable de la Commission Nationale pour la Protection des Données, il est aussi fondamental que cette dernière vérifie la compatibilité des finalités des différents traitements. L'autorisation préalable ne doit pas être considérée comme une simple formalité.

Ainsi, l'interconnexion ne devrait être possible qu'à la condition que les finalités des différents fichiers soient compatibles entre elles. La Chambre de Commerce souhaite que le régime du secret professionnel auquel sont soumises certaines professions soit respecté et qu'ainsi il ne soit pas autorisé d'interconnecter des fichiers gérés par des personnes différentes, particulièrement lorsque celles-ci ne sont pas soumises au même régime de secret professionnel. Rien ne justifierait que les fichiers de l'administration fiscale et ceux de la sécurité sociale soient rapprochés. De même, il ne serait pas concevable que puissent être connectés les fichiers d'établissements de crédit différents. Il appartient, sinon à la loi, du moins à la Commission Nationale pour la Protection des Données d'y veiller.

Des raisonnements analogues doivent prévaloir en ce qui concerne la communication d'informations à des tiers.

Par ailleurs, en ce qui concerne la nécessité d'une autorisation préalable pour l'interconnexion de données à caractère personnel, la Chambre de Commerce rappelle que l'article 11 de la loi sur le contrat d'assurance relatif à l'obligation de déclaration, dispose que „*le preneur ne doit pas déclarer à l'assureur les circonstances déjà connues de celui-ci*". Dans la pratique, afin de connaître les éléments déjà déclarés dans le cadre d'un autre contrat d'assurance auprès du même assureur, ce dernier sera obligé de procéder de façon quasi systématique à des interconnexions de fichiers (pour lesquelles il devra solliciter une autorisation).

De cette façon, la formule dérogatoire de l'autorisation préalable deviendrait le droit commun en matière d'assurance contrairement à l'objectif poursuivi par le législateur qui consiste à simplifier et à alléger la procédure.

7. Des dispositions difficilement applicables

7.1. *La sécurité dans le secteur financier*

En ce qui concerne les traitements à des fins de surveillance, la Chambre de Commerce voudrait faire remarquer que les banques effectuent une surveillance systématique par caméra-vidéo de leurs agences et lieux de distribution de billets de banque. Cette surveillance est effectuée dans un but de protection des personnes concernées ainsi que de prévention des infractions. Le projet de loi adopte à cet égard une attitude tout à fait réaliste en autorisant le traitement à des fins de surveillance dans tous les lieux accessibles au public et en particulier dans les banques. Toutefois, les conditions dans lesquelles celui-ci doit être mis en oeuvre sont par contre tout à fait irréalistes. Si le fait d'apposer des panneaux de signalisation est praticable dans les agences bancaires, l'obligation d'information prévue à l'article 26 du projet de loi est difficile, voire impossible à respecter. En effet, il ne sera pas possible aux banques de communiquer à toutes les personnes qui fréquentent une agence bancaire ou plus encore un simple guichet de retrait d'espèces, qui ne sont pas toujours des clients de la banque en question, les informations requises par l'article 26 du projet de loi. Par conséquent, la Chambre de Commerce demande que les termes „*sans préjudice du droit à l'information prévu à l'article 26*" soient biffés au paragraphe 2 de l'article 10 du projet de loi. Il en est de même du paragraphe 4 de ce même article, qui réitère l'obligation d'information de l'article 26 du projet de loi.

7.2. *La notification à la Commission*

En ce qui concerne l'obligation de notification, la Chambre de Commerce considère que le traitement qui est fait par les banques quant aux données relatives à leurs clients constitue un traitement unique et n'est donc soumis qu'à une seule notification, même si les données sont par la suite réparties entre les différents services de la banque. En effet, d'une part, la collecte est le plus souvent réalisée au moment de l'entrée en relations d'affaires, et, d'autre part, même si l'information est relayée à l'intérieur de l'établissement, d'un service à un autre, elle a été collectée dans un but unique qui est l'exécution du contrat général de fourniture de services qui lie le client à sa banque. Ceci correspond d'ailleurs à la définition du terme „*fichier*" qui vise tout ensemble de données, peu importe que cet ensemble soit ou non centralisé.

7.3. *L'obligation de rectification et/ou de suppression des données*

L'article 28 (5) du projet de loi analysé prévoit l'obligation pour le responsable du traitement de procéder à la rectification, l'effacement ou le verrouillage des données en raison de leur caractère incomplet ou inexact. Aux yeux de la Chambre de Commerce, une interprétation stricte de cette disposition conduirait à une contradiction entre cette obligation de rectification et l'obligation qui résulte de l'article 1334 du Code civil et du règlement grand-ducal du 22 décembre 1986 selon lesquels une copie fidèle consiste en une reproduction indélébile de l'original, protégée contre toute altération. Pour se conformer à ces textes, beaucoup d'entreprises mettent en place des procédures de conservation de leurs archives rendant impossible l'effacement ou la modification des données conservées sur certains supports.

Pour cette raison, la Chambre de Commerce prône une interprétation plus souple permettant aux responsables de traitement de satisfaire aux obligations de l'article 28 (5) du projet de loi sous analyse au moyen d'un ajout réalisé selon une méthode d'archivage identique au traitement antérieur et retraçable lors de la consultation.

7.4. *Le droit d'opposition*

Le droit d'opposition de la personne concernée par un traitement, prévu par l'article 30, est limité dans les hypothèses où le traitement est imposé en vertu de dispositions légales. La Chambre de Commerce attire l'attention sur le fait qu'en pratique, la très grande majorité des traitements tient à une exigence légale (tenue de comptabilité, exigences du droit du travail ou du droit fiscal, …). A défaut de base légale pour un traitement, notamment en ce qui concerne les associations sans but lucratif privées, le juge devra alors faire la difficile appréciation de ce qui est une „*raison prépondérante et légitime*".

7.5. *Le droit à l'information*

Le droit à l'information (article 26 du projet de loi sous examen) concrétise le principe de la bonne foi ou de la transparence du traitement de données à caractère personnel.

En matière d'assurances, la Chambre de Commerce se demande si, p. ex. concernant la gestion de sinistres, l'assureur qui propose une couverture de la responsabilité civile en matière automobile et qui reçoit des données relatives à la victime par un autre assureur, auprès duquel la victime est assurée, doit informer cette victime qu'il a enregistré des données la concernant. Il faut savoir que, de toute façon, et conformément à l'article 26 paragraphe (1) du projet de loi cette victime est déjà informée, au moment de la collecte, par son propre assureur, notamment en ce qui concerne les tiers ou catégories de tiers auxquels les données sont susceptibles d'être communiquées.

L'article 26 paragraphe (3) du projet de loi prévoit que l'information de la personne concernée (dans l'hypothèse où la collecte des données ne s'est pas faite auprès d'elle) n'est pas nécessaire si celle-ci a déjà été informée.

Dans le cas de figure décrit ci-dessus, la Chambre de Commerce estime que l'information donnée par l'assureur de la personne concernée devrait être considérée comme suffisante.

La solution contraire serait à l'origine d'une surcharge de travail considérable pour l'assureur sans apporter une protection supplémentaire à la personne concernée en raison du devoir d'information incombant déjà à son propre assureur. Une information multiple, abstraction faite du coût, ne fera qu'accentuer la méfiance du public vis-à-vis du traitement de données personnelles.

8. Un texte maladroit

Aux yeux de la Chambre de Commerce le texte dans sa teneur et sa présentation actuelle est à revoir. En effet, le texte dans sa version actuelle est indigeste et laisse le lecteur mal à l'aise, qui, intimidé par le nombre impressionnant de sanctions pénales, a des difficultés à se retrouver parmi les différentes dispositions et à se situer dans le cadre qui le concerne personnellement. Les nombreux renvois ne contribuent guère à un éclaircissement du justiciable et sont contraires au principe de droit pénal qui veut que seuls des textes clairs et limpides prévoyent des sanctions.

Certaines dispositions traitent de cas de figure apparemment similaires, mais sont sanctionnées par des peines pénales différentes et parfois illogiques. La Chambre de Commerce renvoie à cet égard à l'article 12 (3) et (4) du projet de loi et s'interroge sur le sens de cette différence. Au vu de ces textes, la Chambre de Commerce se demande si un responsable de traitement ne préférera pas ne pas notifier, plutôt que de se voir exposer au risque d'avoir sciemment fourni des informations incomplètes ou inexactes et de courir ainsi le risque d'une peine de prison.

La même remarque vaut en ce qui concerne l'article 13 (4) du projet de loi sous analyse qui punit le non-respect des paragraphes 1er et 2 du même article. L'article 13 (1) énumère un certain nombre d'informations que doit comprendre la notification et l'article 13 (2) prescrit la notification de toute modification d'une de ces informations. La Chambre de Commerce ne saisit pas la différence entre l'infraction sanctionnée par l'article 13 (4) et celle punie par l'article 12 (3), respectivement 12 (4).

Par ailleurs, le texte contient un certain nombre de doubles emplois. Plus particulièrement, la Chambre de Commerce attire l'attention des auteurs du projet de loi à cet égard sur les articles 7 (2) et 14 (1) (a), ainsi que sur les articles 14 (1) (c) et 16 (1).

En ce qui concerne le traitement à des fins de surveillance sur le lieu de travail (article 11 du projet de loi), la Chambre de Commerce voudrait faire remarquer que l'emploi du mot „légitime" à l'article 11 (1) *in fine*, n'est pas correct. Il faudrait en effet remplacer le mot „*légitime*" par le mot „*licite*", alors que le traitement mis en oeuvre devra de toute façon être légitime et rentrer dans un des six cas prévus par l'article 5 du projet de loi.

Certaines questions restent encore ouvertes. Ainsi, par exemple, concernant l'article 18 du projet de loi sous examen, la Chambre de Commerce s'interroge sur les pouvoirs réels de la Commission nationale. En effet, aux termes de l'article 25.6, deuxième alinéa, de la directive 95/46/CE, les Etats membres prennent les mesures nécessaires pour se conformer à la décision de la Commission européenne lorsque celle-ci constate qu'un pays tiers assure un niveau de protection adéquat en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes. En d'autres termes, un tel constat de la part de la Commission européenne du niveau adéquat lie les Etats membres. Une telle obligation de la part des Etats membres ne ressort pas clairement du projet de loi et la Chambre de Commerce se pose en conséquence la question quelle est la marge de manoeuvre des commissions nationales.

En ce qui concerne ce même article 18, la Chambre de Commerce aimerait préciser qu'il y a lieu d'ajouter le bout de phrase „*ou destinées à faire l'objet d'un traitement*" au paragraphe (1) après le début de phrase „*Le transfert de données faisant l'objet d'un traitement …*".

Finalement, il y a lieu de reformuler l'article 24 (3) du projet de loi comme suit: „*Le prestataire de service de certification ne peut opposer à la Commission le secret professionnel auquel il est soumis conformément à l'article 19 de la loi du 14 août 2000 relative au commerce électronique*", terme consacré par l'article 72 de ladite loi.

9. Conclusion

Il est clair que les Etats européens n'ont qu'une faible marge de manoeuvre en ce qui concerne la transposition de la directive 95/46/CE. Le Luxembourg se doit de ce fait de respecter les principes de base de cette directive. En particulier, le principe de finalité est, dans l'optique communautaire, à la base de la protection des personnes à l'égard des traitements de données. La Chambre de Commerce se permet de souligner à cet égard que l'interconnexion des fichiers ne doit pas permettre d'introduire une brèche dans ce principe.

Une interprétation stricte des dispositions du projet de loi dans sa version actuelle conduit vers une situation telle que tout rassemblement de données quelconques, si anodines soient-elles, et tout traitement, si élémentaire soit-il, est soit soumis à autorisation, soit prohibé.

La Chambre de Commerce exprime son accord avec une meilleure protection de la vie privée. Toutefois, elle ne peut s'exprimer en faveur des multiples tracasseries administratives que suscite le projet de loi. A défaut d'assouplir la rigueur des exigences prévues, le texte projeté risque de n'être guère plus viable que la loi du 31 mars 1979 et de rester tout aussi largement ignoré, ceci d'autant plus que la présentation et la rédaction actuelle du projet de loi sont assez indigeste et maladroite.

*

La Chambre de Commerce, après consultation de ses ressortissants, ne peut donc approuver le projet de loi sous rubrique dans sa version actuelle.

Service Central des Imprimés de l'Etat

4735/07

N° 4735[7]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

RAPPORT POUR AVIS DE LA COMMISSION DU TRAVAIL ET DE L'EMPLOI

(15.5.2002)

La Commission se compose de: M. Marcel GLESENER, Président-Rapporteur pour avis; MM. François BAUSCH, Xavier BETTEL, Niki BETTENDORF, Aloyse BISDORFF, Aly JAERLING, Nico LOES, Lucien LUX, Paul-Henri MEYERS, Patrick SANTER, Théo STENDEBACH et Marc ZANUSSI, Membres.

*

INTRODUCTION

La Commission du Travail et de l'Emploi a examiné le projet de loi 4735 dans ses aspects concernant le droit du travail, c'est-à-dire principalement l'article 11 réglementant le traitement des données à des fins de surveillance sur le lieu de travail.

Dans sa réunion du 8 février 2001, la commission a procédé à un premier échange de vues général sur le texte de l'article 11 et elle a désigné son président M. Marcel Glesener comme rapporteur pour avis. Dans ses réunions des 3 et 10 mai 2002, la commission a examiné l'avis du Conseil d'Etat et des avis des chambres professionnelles avant d'adopter à l'unanimité le présent rapport pour avis dans sa réunion du 15 mai 2002. Les recommandations formulées par la commission dans le présent avis à l'intention de la Commission des Média et des Communications, saisie pour rapport du projet de loi 4735, ont été élaborées en étroite concertation avec M. François Biltgen, Ministre du Travail et de l'Emploi et Ministre délégué aux Communications.

*

TRAITEMENT DE DONNEES A DES FINS DE SURVEILLANCE SUR LE LIEU DE TRAVAIL: ARTICLE 11 DU PROJET DE LOI

L'article 11 permet à l'employeur de surveiller sous certaines conditions ses employés sur le lieu de travail. Le texte tient ainsi compte de certaines pratiques qui se sont progressivement développées au cours des dernières années sur le lieu de travail. Il se propose d'encadrer ces techniques légalement, tout en apportant des garanties nécessaires aux droits des travailleurs. Voilà pourquoi, la surveillance sur le lieu de travail est soumise à des conditions assez strictes.

Le paragraphe (1) du texte gouvernemental prévoit quatre cas d'ouverture, où cette surveillance est permise;

a) pour des besoins de sécurité et de santé des travailleurs;

b) pour les besoins de protection des biens de l'entreprise;

c) pour le contrôle du processus de production portant uniquement sur les machines;

d) pour le contrôle temporaire de production ou des prestations du travailleur en vue de mesurer son activité afin de déterminer sa rémunération.

Ce texte précise encore que, pour les cas visés aux points a) et d), le comité mixte d'entreprise a un pouvoir de décision. Par ailleurs, le consentement exprès de la personne concernée ne permet pas d'outrepasser les conditions légales auxquelles est soumise la mise en oeuvre du traitement.

Le paragraphe (2) prévoit que le comité mixte ou à défaut la délégation du personnel ou à défaut encore l'Inspection du travail et des mines sont informés par l'employeur de la finalité du traitement auquel les données sont destinées et de la ou des périodes de surveillance ainsi que de la durée de conservation des données.

*

AVIS DU CONSEIL D'ETAT ET DES CHAMBRES PROFESSIONNELLES

Il est utile de retracer très brièvement l'orientation générale des avis du Conseil d'Etat et des chambres professionnelles.

Le Conseil d'Etat constate qu'en principe les dispositions de l'article 11 sont destinées à s'appliquer tant au secteur public qu'au secteur privé. Or, comme ni le comité mixte d'entreprise, ni l'Inspection du travail et des mines ne sont compétents en matière de relation de travail dans le secteur public, l'article 11 du projet de loi ne pourra donc trouver application dans le secteur public. Le Conseil d'Etat en déduit qu'il y a lieu d'éliminer l'article 11 du présent projet de loi et d'approfondir la problématique en la plaçant dans un contexte plus général.

La Chambre des Fonctionnaires et Employés publics relève la même problématique en soulignant que l'article 11 se heurte au statut général des fonctionnaires de l'Etat, alors que, notamment, ce statut ne permet pas de mesurer la productivité du fonctionnaire afin de déterminer sa rémunération.

La Chambre de Travail s'oppose énergiquement à l'introduction de tout genre de moyens de surveillance électronique ou numérique, alors qu'il lui paraît impossible de l'instaurer pour des finalités limitées et déterminées. Elle estime que la surveillance électronique constitue par définition un instrument disproportionné au but recherché par l'employeur. Elle craint de nombreux abus risquant de rejeter le salarié à la merci des employeurs.

La Chambre des Métiers accueille favorablement l'introduction du droit de l'employeur de surveiller sous certaines conditions les salariés sur le lieu de travail. Elle est cependant d'avis que le texte de l'article 11 ne revêt pas le caractère de précision et de clarté nécessaires. Elle soulève par ailleurs le problème du contrôle par l'employeur de l'utilisation à des fins privées du matériel informatique mis à disposition des salariés (Internet et messagerie électronique).

Dans sa prise de position très nuancée, la Chambre des Employés privés souligne qu'il s'agit de trouver un équilibre entre la possibilité de surveillance des employés et le respect de la liberté de leurs droits fondamentaux. Elle considère toutefois que les conditions de la mise en oeuvre de la surveillance devraient être précisées afin d'éviter des abus. Ainsi des représentants du personnel devraient disposer d'un moyen de contrôle sur la finalité de la surveillance et sur l'usage fait des données recueillies. La Chambre professionnelle critique également le fait que le projet de loi limite le pouvoir de décision du comité mixte à deux des quatre cas d'ouverture où la surveillance est permise.

*

DECISION DE PRINCIPE CONCERNANT LA NECESSITE DE LEGIFERER

La commission a été informée que le Gouvernement rejette la proposition du Conseil d'Etat de supprimer purement et simplement l'article 11 en attendant une réglementation plus générale de l'utilisation et du traitement du matériel informatique sur le lieu de travail.

Bien que la directive 95/46/CE relative à la protection des données à caractère personnel ne traite pas particulièrement cette question, le Gouvernement estime qu'il est opportun et nécessaire de saisir l'occasion de la transposition de cette directive pour encadrer légalement le traitement de données à des fins de surveillance sur le lieu de travail.

La commission rappelle que certaines affaires concernant des surveillances sur le lieu de travail ont été rendues publiques et ont donné lieu à de vives contestations. Ainsi la presse s'est fait l'écho d'un cas de surveillance mise en place dans une grande surface à l'insu du personnel. Ce cas concret a donné lieu à une question parlementaire et au vu de la réponse du Ministre du Travail et de l'Emploi, la nécessité d'une intervention législative est apparue au grand jour.

En effet, en l'état actuel du droit, le salarié dispose d'une protection tout à fait insuffisante pour s'opposer aux nombreuses formes de surveillance électronique abusives dont il peut faire l'objet sur le lieu de travail.

En réalité, l'employeur peut laisser libre cours à son imagination dans ce domaine. Par contre le salarié ne peut s'opposer à des abus que pour autant qu'il arrive à fournir la preuve que les moyens de surveillance mis en oeuvre comportent une intrusion illicite dans sa vie privée et qu'il est donc victime d'une atteinte à la vie privée conformément à la loi du 11 août 1982 concernant la protection de la vie privée. La finalité de l'intervention législative est donc d'apporter un surplus de sécurité juridique, alors que le cadre juridique actuel, s'il n'est pas inexistant, est toutefois loin de donner satisfaction.

Au plan européen un groupe de travail a été institué pour analyser les réponses à donner à l'ensemble de la problématique posée d'une façon générale par l'usage des instruments et moyens de communication informatiques sur le lieu de travail. Cette problématique englobe notamment l'utilisation par le salarié de l'Internet à des fins privées et la question de savoir si l'employeur a le droit de contrôler le courrier électronique des salariés. Or, vu l'état actuel d'avancement de ces travaux, il ne faudrait pas s'adonner à l'illusion que la réglementation légale de ce cadre plus général puisse encore se faire pendant la présente législature. Supprimer l'article 11 dans le présent projet équivaudrait dès lors à continuer à laisser les salariés sans protection efficace contre toute sorte d'abus auxquels la surveillance sur le lieu de travail peut actuellement donner lieu.

La nécessité d'une intervention législative pour réglementer la surveillance du lieu de travail se vérifie encore par rapport au télétravail, d'une part, pour éviter toute forme d'intrusion dans la vie privée du salarié et, d'autre part, pour éviter qu'en l'absence de mesurage du temps de travail presté par le salarié à domicile, il puisse se faire exploiter.

Compte tenu de toutes ces considérations, il paraît indispensable de trancher d'abord la question de principe de savoir si oui ou non une intervention législative dans le cadre du présent projet de loi est opportune.

A la suite d'une réflexion approfondie, la commission s'est dit convaincue de la nécessité de légiférer dans les meilleurs délais, ceci avec la finalité d'instituer une protection efficace du salarié lui conférant toutes les garanties nécessaires pour faire respecter ses droits dans ce domaine. L'intervention législative s'impose alors qu'actuellement au Luxembourg aucun texte légal ne fixe clairement les limites dans lesquelles un employeur peut surveiller ses salariés sur le lieu de travail. La loi du 11 août 1982 concernant la protection de la vie privée peut trouver application dans certaines hypothèses (voir ci-dessus), mais il faut être conscient du fait qu'elle ne vise en aucun cas directement et de façon générale la protection des droits des salariés. Il s'agit dès lors de voir de quelle façon le texte de l'article 11 pourra être amendé pour répondre efficacement à sa finalité de protection des salariés, notamment en rencontrant les appréhensions exprimées dans les avis précités. Il faudra s'assurer que l'intervention législative comporte effectivement une amélioration par rapport à la situation juridique actuelle. Dans cette optique, le texte légal devra écarter tout moyen de trouver, par la voie de subterfuges plus ou moins ingénieux, de nouvelles possibilités d'abus au détriment des salariés.

*

PROPOSITIONS CONCERNANT LE TEXTE DE L'ARTICLE 11

Cette décision de principe acquise, la commission a procédé à l'examen détaillé du texte de l'article 11.

a) Paragraphe (1)

Parmi les cas d'ouverture à la mise en oeuvre d'une surveillance sur le lieu de travail, c'est le point (d) qui pose le plus problème. Ce point est libellé comme suit:

„(d) pour le contrôle temporaire de production ou des prestations du travailleur en vue de mesurer son activité afin de déterminer sa rémunération.“

Le Gouvernement a proposé de remplacer les termes *„en vue de mesurer son activité afin de déterminer sa rémunération“* par le bout de phrase *„lorsqu'une telle mesure est nécessaire pour déterminer la rémunération“*.

La commission estime que pour renforcer encore le caractère restrictif de ce cas d'ouverture et pour en souligner la finalité de protection des travailleurs, il serait préférable d'écrire *„… lorsqu'une telle mesure **est le seul moyen** pour déterminer la rémunération **exacte***“. Ce n'est donc qu'en l'absence d'autres moyens pour déterminer la rémunération **exacte** des salariés que ce cas d'ouverture pourrait s'appliquer.

En précisant que cette mesure n'est possible que pour autant qu'elle vise à déterminer la rémunération **exacte** du salarié, la commission entend encore restreindre le champ d'application de ce cas d'ouverture, alors qu'il est clair que l'opération de surveillance y visée ne saurait aucunement avoir pour effet de remettre en cause le principe du mode de rémunération du salarié et qu'elle ne peut donc viser que des détails concernant éventuellement des éléments accessoires de la rémunération.

La commission a également évoqué certaines réserves de principe formulées à l'encontre de ce cas d'ouverture selon lesquelles ce texte pourrait indirectement valoir comme légitimation pour les employeurs du système d'évaluation des performances. Selon ces critiques, les employeurs, forts de la consécration légale de ce système, pourraient abusivement en déduire la nécessité d'installer systématiquement des caméras de surveillance.

La commission considère que cette approche doit céder le pas par rapport à la nécessité impérieuse d'encadrer légalement des procédés qu'on ne saurait prohiber totalement et qui actuellement s'exercent en l'absence de toute règle de protection pour le salarié.

Toutefois, dans le souci de tenir compte des nombreuses craintes exprimées au sujet de la mise en oeuvre de ce texte, la commission considère qu'il y a lieu d'en dresser un bilan après un certain délai d'application. Ce bilan pourrait, le cas échéant, être effectué dans le cadre de la révision de la loi „PAN“.

Afin de tenir compte des dispositions spécifiques existant dans le cadre de la fonction publique et de la législation PAN, la commission reprend la proposition du Gouvernement d'ajouter au paragraphe (1) un cas d'ouverture supplémentaire ainsi libellé:

„(e) dans le cadre d'une organisation de travail selon l'horaire mobile conformément à la loi.“

La commission est d'avis que ce point (e) doit être ajouté aux cas visés aux lettres (a) et (d) pour lesquels le comité mixte d'entreprise a un pouvoir de décision tel que défini à l'article 7 paragraphes 1 et 2 de la loi du 6 mai 1974 sur les comités mixtes dans les entreprises du secteur privé.

La commission rappelle que la finalité première de l'intervention du comité mixte doit être d'assurer que les principes de proportionnalité et de fonctionnalité soient en tout état de cause respectés dans la mise en oeuvre de la procédure de surveillance.

Dans cet ordre d'idées, la commission s'est interrogée sur l'opportunité de prévoir la décision du comité mixte également pour les points (b) et (c) concernant respectivement les besoins de protection des biens de l'entreprise et le contrôle du processus de production portant uniquement sur les machines. Or, dans la mesure où les attributions prévues aux points (b) et (c) ne semblent pas rentrer dans les domaines où le comité mixte d'entreprise a compétence de décision conformément à l'article 7 précité de la loi du 6 mai 1974, il faudrait prévoir dans le cadre du présent projet une disposition modificative de cette loi de base sur les comités mixtes.

La commission considère cependant que cette option de modifier dans le cadre du présent projet de loi concernant la protection des personnes à l'égard du traitement des données à caractère personnel une autre loi importante relevant du domaine de la cogestion, donc d'un domaine tout à fait étranger au projet de loi, constituerait une méthode législative critiquable et qui, en régie générale, se heurte aussi à l'opposition du Conseil d'Etat.

Cette argumentation a finalement amené la commission à renoncer à la proposition de conférer au comité mixte un pouvoir de décision pour les cas d'ouverture prévus aux points (b) et (c).

Toutefois, en se référant notamment aux questions soulevées par la Chambre des Employés privés au sujet des moyens d'action des représentants du personnel en cas d'abus de l'employeur, la commission propose d'insérer dans le texte de l'article 11 un **paragraphe (3) nouveau** prévoyant que la personne concernée ainsi que tous les organes intervenant dans le cadre de la procédure prévue au paragraphe (2) peuvent saisir la commission nationale pour la protection des données lorsqu'ils ont des doutes sur le

respect des dispositions de l'article 11. Dans cette hypothèse, la commission nationale serait obligée de statuer endéans un délai à déterminer, dans le cadre des possibilités de sanctions lui conférées par l'article 35. Le texte devrait encore préciser que cette procédure de saisine de la commission nationale se fait sans préjudice des attributions de l'Inspection du travail et des mines.

L'alinéa final du paragraphe 1 de l'article 11 prévoit une disposition particulièrement importante, à savoir que le consentement exprès de la personne concernée ne rend pas légitime le traitement mis en oeuvre par l'employeur. En d'autres termes, le salarié ne saurait renoncer pour quelque raison que ce soit à la protection légale.

La commission propose de supprimer le terme „exprès" comme étant superfétatoire, alors que le concept du „consentement de la personne concernée" a été défini au point (1) de l'article 2 du projet de loi.

Compte tenu des modifications ci-dessus exposées, la commission propose de donner au paragraphe (1) la teneur suivante:

„(1) Le traitement à des fins de surveillance sur le lieu de travail peut être mis en oeuvre, conformément à l'article 14, par l'employeur s'il en est le responsable. Un tel traitement n'est possible que s'il est nécessaire:

(a) pour les besoins de sécurité et de santé des travailleurs, ou

(b) pour les besoins de protection des biens de l'entreprise, ou

(c) pour le contrôle du processus de production portant uniquement sur les machines, ou

(d) pour le contrôle temporaire de production ou des prestations du travailleur, ***lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte, ou***

(e) dans le cadre d'une organisation de travail selon l'horaire mobile conformément à la loi.

Dans les cas visés aux lettres (a), (d) ***et (e)****, le comité mixte d'entreprise, le cas échéant institué, a un pouvoir de décision tel que défini à l'article 7 paragraphes (1) et (2) de la loi du 6 mai 1974 instituant des comités mixtes dans les entreprises du secteur privé et organisant la représentation des salariés dans les sociétés anonymes. Le consentement* ~~***exprès***~~ *de la personne concernée ne rend pas légitime le traitement mis en oeuvre par l'employeur."*

b) paragraphe (2)

La commission propose de donner à ce paragraphe la teneur suivante:

„Sans préjudice du droit à l'information de la personne concernée ***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.***"

Ce texte tient compte des critiques exprimées par le Conseil d'Etat et par la Chambre des fonctionnaires et employés publics, concernant l'impossibilité d'appliquer l'article 11 dans sa teneur initiale à la fonction publique. Les amendements y apportés ont pour objet d'étendre l'obligation d'information de l'employeur également aux organismes de représentation du personnel tombant sous le statut général des fonctionnaires de l'Etat ou d'un autre régime statutaire.

Luxembourg, le 15 mai 2002

Le Président-Rapporteur pour avis,
Marcel GLESENER

Service Central des Imprimés de l'Etat

4735/08

N° 4735[8]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

AMENDEMENTS ADOPTES PAR LA COMMISSION DES MEDIAS ET DES COMMUNICATIONS

DEPECHE DU PRESIDENT DE LA CHAMBRE DES DEPUTES AU PRESIDENT DU CONSEIL D'ETAT

(6.6.2002)

Monsieur le Président,

Me référant à l'article 19 (2) de la loi du 12 juillet 1996 portant réforme du Conseil d'Etat, j'ai l'honneur de vous soumettre ci-après une série d'amendements au projet de loi sous rubrique, amendements adoptés par la Commission des Médias et des Communications lors de sa réunion du 5 juin 2002, en présence de M. le Ministre délégué aux Communications qui a apporté l'avis favorable du Gouvernement.

Afin de faciliter l'examen des modifications, elles ont de suite été intégrées dans le texte qui fait ainsi fonction de texte coordonné.

Chapitre 1. – ***Dispositions générales relatives à la protection de la personne à l'égard des traitements des données à caractère personnel***

Art. 1er. – ***Objet***

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 et fait respecter les intérêts légalement protégés des personnes morales.

Commentaire:

Reprise partielle du texte du Conseil d'Etat. Le texte est plus cohérent par rapport à celui de la directive. Toutefois, „la protection légale de la personne morale" est une expression plus restrictive que celle „d'intérêt légitime" utilisé dans la directive.

Art. 2. – ***Définitions***

Aux fins de la présente loi, on entend par:

(a) (~~m~~) „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) (~~p~~) „Commission nationale": la Commission nationale pour la protection des données.

(c) (~~l~~) „consentement de la personne concernée": toute manifestation de volonté expresse, non équivoque, 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) (~~k~~) „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 d'une mission d'enquête particulière~~ dans le cadre de l'exécution d'une mission légale d'enquête ou de contrôle ne sont pas considérées comme des destinataires;

(e) (~~a~~) „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 ou morale est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique;

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

(g) (~~r~~) „donnée génétique": toute donnée concernant les caractères héréditaires d'un individu ou d'un groupe d'individus apparentés;

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

(i) (~~q~~) „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;

~~personne physique ou morale autorisée à exercer soit des activités ayant pour objet la prévention, le diagnostic ou le traitement de maladies et infirmités, soit des activités de soins, soumise au secret professionnel au sens de l'article 458 du code pénal;~~

(j) (~~e~~) „interconnexion": toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour une autre finalité par le même responsable du traitement ou par un ou d'autres responsables du traitement;

(k) (~~f~~) „ministre": le ministre ayant dans ses attributions la protection des données;

(l) (~~r~~) „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, ainsi que des prestations familiales ou d'aides sociales.

(m) (~~o~~) „pays tiers": Etat non membre de l'Union européenne;

(n) (~~b~~) „personne concernée": toute personne physique ou morale, publique ou privée ou groupement de fait ~~sujet~~ qui fait l'objet d'un traitement de données à caractère personnel;

(o) (~~g~~) „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;

(p) (~~i~~) „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;

(q) (~~h~~) ~~„surveillance": toute activité faisant appel à des moyens techniques en vue de détecter, d'observer et/ou de copier et/ou d'enregistrer intentionnellement les mouvements et/ou les paroles et/ou les écrits et/ou l'état d'un objet ou d'une personne fixe ou mobile;~~

„surveillance": 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;

(r) (j) „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;

(s) (e) „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.

Commentaires:

La commission a procédé à un réagencement des définitions. Celles-ci ne sont plus indiquées par ordre d'apparence dans le texte du projet, mais par ordre alphabétique, ce qui permet une recherche plus aisée.

(a) „code de conduite“: Rejet de la proposition du Conseil d'Etat et maintien de la définition initiale. Même si la valeur juridique de cette définition est de nature conventionnelle; il n'en demeure pas moins que sa présence au sein du projet de loi lui offre une reconnaissance dont l'utilité pratique est indéniable en la matière. Conformément à la définition de la Commission nationale visée au point (b), l'adjectif „nationale“ a été rajouté tout au long du projet de loi.

(b) „Commission nationale“, (c) „consentement de la personne concernée“, (d) „destinataire“, (f) „donnée relative à la santé“ et (g) „donnée génétique“: Reprise du texte du Conseil d'Etat

(h) „fichier de données à caractère personnel“: La modification correspond à un alignement du texte avec celui de la directive. L'élimination de la référence aux fichiers non structurés ne peut se faire que sous réserve de ne pas contourner la loi. Dans cet ordre d'idées rappelons que collecter des données exige que:

– la collecte soit légitime

– la collecte corresponde à une ou plusieurs finalités déterminées.

De ce fait on ne collecte pas de données à caractère personnel sans avoir une idée précise en tête. Pour s'aligner sur le texte de la directive, il y a donc lieu d'exclure les fichiers non structurés du champ d'application du projet de loi tout en précisant que dès lors qu'un fichier retrouve une structure quelconque il retombera sous le champ de la loi.

(i) „instance médicale“: Reprise partielle du texte du Conseil d'Etat. L'adoption pure et simple de la définition proposée par le Conseil d'Etat aurait pu faire surgir une contradiction entre d'une part l'article 7 (1), qui exclurait les personnes morales, dont les hôpitaux, et d'autre part l'article 7 (3) qui, loin de les exclure fait bénéficier les hôpitaux d'une procédure simplifiée. En outre, l'adoption de la définition proposée par le Conseil d'Etat fait apparaître que d'autres organismes tels que la Croix-Rouge, la Ligue luxembourgeoise de Prévention et d'action médicosociales qui traitent des données médicales à bon droit, au vu et su du gouvernement et avec la participation financière, risquent de tomber dans l'illégalité, alors que ce ne sont pas des instances médicales, du moins pas dans la définition qu'en donne le Conseil d'Etat, ni des organismes de la Sécurité Sociale ou administrations au sens de l'article 7 (1).

L'article 7 (1) va être adapté en conséquence.

(n) „personne concernée“: Reprise de la proposition du Conseil d'Etat et ajout des groupements de fait pour ne pas faire dépendre l'application de la loi à l'existence de la personnalité juridique.

(q) „surveillance“: Reprise du texte du Conseil d'Etat

Art. 3. – *Champ d'application*

(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.

(2) Sont soumis à la présente loi:

(a) le traitement mis en oeuvre par un responsable du traitement soumis au droit luxembourgeois;

(b) le traitement

– dont le responsable du traitement est établi sur le territoire luxembourgeois ou
– dont le responsable du traitement, 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.

Par 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 s'applique 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.

(4) La présente loi s'applique à toute forme de captage, de traitement et de diffusion de sons et images qui permettent d'identifier des personnes physiques ou morales.

(5) 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
– au traitement de données concernant une personne morale et dont la publication est prescrite par une loi ou un règlement.

Commentaires:

2 (a): Reprise du texte du Conseil d'Etat avec une modification de pure forme

2 (b): La rédaction initiale de l'article 3 paragraphe 2 lettre b) ne satisfait pas à l'exigence de clarté de la législation et prête à confusion. En effet, l'hypothèse du traitement aux seules fins de transit est exclusive de l'obligation de désigner un représentant sur le territoire luxembourgeois et non le contraire.

(3): Reprise de la proposition du Conseil d'Etat de recaler le paragraphe (3) à la fin de l'article 3 lequel devient alors un paragraphe (5).

Le texte du nouveau paragraphe (3) en lui-même restera inchangé par rapport au texte initial. L'ajout de l'adjectif „national" à la „défense" n'a pas été reprise. Il n'y a pas de Ministre de la Défense Nationale, mais un Ministre de la Défense.

(4): Rejet de la proposition du Conseil d'Etat de supprimer le paragraphe (4). Il a été jugé utile de préciser, comme il résulte du considérant 14 de la directive 95/46, que dans le cadre de la société de l'information, les techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images tombent également sous le champ d'application de la présente loi.

(5) Le premier tiret est la reprise du paragraphe (3) du texte initial. Le second tiret a pour objet de permettre le traitement libre, pour toute personne, de données dont la loi ou un règlement exige qu'elles soient mises à disposition du public, en particulier celles publiées au Mémorial. Cette exclusion s'avère nécessaire compte tenu du champ d'application très large du projet de loi lequel englobe également la protection des données relatives aux personnes morales.

Chapitre II. – *Conditions de licéité du traitement*

Art. 4. – *Qualité des données*

(1) Le responsable du traitement doit s'assurer ~~garantir~~ 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) ~~de l'alinéa~~ ci-après.

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

(3) Quiconque effectue un traitement en violation des dispositions du présent ~~de cet~~ article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ~~10.001 à 3.000.000 LUF~~ ou d'une de ces peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.

Commentaires:

(1): Reprise partielle du texte du Conseil d'Etat. Outre la modification de pure forme. La référence au paragraphe (2) dans le point d) vise à faire le lien avec le traitement ultérieur des données à des fins historiques, statistiques ou scientifiques visé au paragraphe (2).

(2): Il s'agit d'une modification rédactionnelle.

(3): Reprise du texte du Conseil d'Etat avec l'ajout que la juridiction répressive peut prononcer la fermeture définitive ou temporaire de l'établissement. Il s'agit d'une infraction matérielle. La présente loi prévoit également des infractions exigeant un dol général (voir p.ex. article 28 (2)). Dans ces derniers cas, l'adverbe „sciemment" a été ajouté.

Art. 5. – ***Légitimité du traitement***

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

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

(b) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, ou si

(c) le traitement 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 si

(d) le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, ou si

(e) le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou si

(f) la personne concernée a donné son consentement ~~exprès~~.

(2) Quiconque effectue un traitement en violation des dispositions du présent ~~de cet~~ article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ~~10.001 à 3.000.000 LUF~~ ou d'une de ces peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.

Commentaires:

Le commerce électronique tombe dans le champ d'application du présent projet de loi. La commission ne partage pas la crainte exprimée par le Conseil d'Etat sur un éventuel „problème de coexistence harmonieuse" entre les deux lois.

(1): Suite à la nouvelle définition de „consentement de la personne concernée" figurant à l'article 2 lettre c), la référence au consentement „exprès" est tautologique. Cette modification est faite dans l'ensemble du texte.

(2): voir sous article 4 (3).

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.

~~Aux fins de la présente loi, on entend par:~~

~~(a) „donnée relative à la santé": toute information concernant l'état physique et mental d'une personne concernée, y compris certaines données génétiques, de même que les informations sociales et administratives connexes susceptibles d'avoir une incidence sur cet état;~~

~~(b) „donnée génétique": toute donnée, quel qu'en soit le type, qui concerne les caractères héréditaires d'un individu ou qui est en rapport avec de tels caractères formant le patrimoine d'un groupe d'individus apparentés.~~

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

(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 ~~où la loi prévoit que l'interdiction visée au paragraphe (1) ne peut être levée par le consentement de la personne concernée~~, ou lorsque

(b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement notamment en matière de droit du travail dans la mesure où il est autorisé par la loi ~~par disposition légale~~, 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 oeuvre, 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 ~~exprès~~ des personnes concernées, ou lorsque

(e) le traitement porte sur des données manifestement rendues publiques par la personne concernée ~~ou dès lors que son consentement au traitement des données peut légitimement être déduit de ses déclarations~~, ou lorsque

(f) le traitement mis en oeuvre conformément aux règles de procédures judiciaires en matière civile applicables est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice s'il est mis en oeuvre à cette fin exclusive, ou lorsque

(g) le traitement s'avère nécessaire pour un motif d'intérêt public ~~important~~ notamment à des fins historiques, statistiques ou scientifiques sans préjudice de l'application de l'article 7 ci-après et que ce traitement est mis en oeuvre conformément au régime d'autorisation préalable de la Commission nationale tel que prévu à l'article 14, ou lorsque

(h) le traitement est mis en oeuvre par voie de règlement grand-ducal tel que prévu à l'article 17.

(3) L'article 6 paragraphe (1) ne s'applique pas lors d'une procédure judiciaire ou d'une enquête pénale. Toutefois les données génétiques ne peuvent être traitées que 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 ~~d'un danger concret~~ ou la répression d'une infraction pénale déterminée.

(4) Par dérogation ~~exception~~ à l'article 6, paragraphe (1), les données génétiques ne peuvent faire l'objet d'un traitement que:

~~(4) Les données génétiques peuvent être traitées:~~

(a) dans les cas visés par les articles 6, paragraphe (2) lettres (c), (f), (g), (h), 6 paragraphe (3) et 7 de la présente loi, ou lorsque

(b) ~~lorsque~~ la personne concernée a donné son consentement ~~exprès~~ et si le traitement est effectué dans les seuls domaines de la santé ou de la recherche scientifique sauf indisponibilité du corps humain et 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.

(5) 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 ~~10.001 à 5.000.000 LUF~~, ou d'une de ces peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du paragraphe (1) du présent article.

Commentaires:

(1): Reprise de la position du Conseil d'Etat de transférer les définitions à l'article 2. En ce qui concerne les termes de „vie sexuelle", il y a lieu de les maintenir alors que, d'une part, il s'agit de termes également utilisés dans la directive et que, d'autre part, la vie sexuelle doit s'entendre comme incluant l'orientation sexuelle.

(2) (a): Reprise de l'expression „le cas interdit par la loi" avancée par le Conseil d'Etat. En revanche il est proposé de maintenir la référence à „l'indisponibilité du corps humain". En matière de données génétiques, le traitement se fait souvent sans dissociation immédiate entre la donnée et son support organique. Lorsqu'on génère la carte du génome d'un sujet, un traitement est constitué. De plus, on peut envisager que les données soient, le cas échéant, saisies à partir de protéines et d'un matériel bio-moléculaire et réutilisés pour reconstituer en grandeur nature le génome du sujet. Une fois cette opération réalisée on est à deux pas du clonage sans avoir jamais utilisé le matériel organique du sujet cloné lui-même. Ainsi semble-t-il opportun de maintenir la référence à „l'indisponibilité du corps humain" afin d'éviter tout risque d'eugénisme et de clonage.

(2) (b), (e) et (f): Reprise du texte du Conseil d'Etat

(2) (g): Si la commission suit le Conseil d'Etat dans sa proposition de supprimer l'adjectif „important" elle se prononce en revanche en faveur du maintien du mot „notamment", car l'article 4 (2) n'a pas le même champ d'application que l'article 6 (2) (g). L'article 4 (2) ne concerne pas les catégories particulières de données de sorte que celui-ci ne permet pas d'élargir le champ de la dérogation pour d'autres motifs d'intérêt public.

(3): L'amendement a pour objet de préciser que seul le domaine pénal est visé. Ainsi peuvent être traitées des données génétiques dans le cadre d'enquêtes sur des personnes trouvées mortes, afin de vérifier si la mort est naturelle ou s'il y a eu infraction pénale.

(4): L'amendement est purement rédactionnel.

(5): L'amendement vise à obtenir un parallélisme avec l'article 7 (5). A l'article 7 (5) la référence à l'article 6 (5) a été supprimée afin d'éviter tout double emploi. Voir aussi sous article 4 (3).

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

(1) Lorsque le traitement de données tel que défini à l'article 6 paragraphe (1) de la présente loi est 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, de la recherche scientifique dans le domaine de la biologie et de la médecine; le traitement de ces données peut être mis en oeuvre 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 ou des mutuelles et par toute personne physique ou morale 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 oeuvrant dans les domaines social, familial et thérapeutique. ~~et lorsque le responsable du traitement est soumis au secret professionnel.~~ Le recours à un sous-traitant est possible dans les conditions ~~de confidentialité~~ prévues à l'article 21.

(2) Le traitement visé ci-dessus ~~à l'article 7 paragraphe (1)~~ fait l'objet d'une autorisation préalable de la Commission nationale.

(3) Par dérogation au paragraphe (2) qui précède ~~est~~ sont soumis à notification:

– le traitement mis en oeuvre conformément à l'article 36 de la loi du 28 août 1998 sur les établissements hospitaliers;
– le traitement mis en oeuvre par un médecin et concernant ses patients.

(4) 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.

~~(4) En application des articles 6 et 7 un règlement grand-ducal établit:~~

~~(a) les modalités et les conditions d'après lesquelles les données visées à l'article 6 paragraphe (1) de la loi peuvent être communiquées à un tiers;~~
~~(b) les modalités et les conditions d'après lesquelles les données visées à l'article 6 paragraphe (1) de la loi peuvent être utilisées à des fins de recherche;~~

(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 ~~10.001 à 5.000.000 LUF~~, ou d'une de ces peines seulement. ~~La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.~~

Commentaires:

(1): Il semble opportun d'inclure les „entreprises d'assurance, les sociétés gérant les fonds de pension et les mutuelles" dans les prévisions de l'article 7 (1) sous peine de leur interdire toute activité. La simple collecte de données relatives à la santé tombe sous le champ de la loi et ne peut être pratiquée que par un organisme à ce autorisé à l'article 7. Or lesdits organismes ne sauraient fonctionner et verser des pensions d'invalidité sans disposer de données relatives à la santé.

(2) et (4): Reprise du texte du Conseil d'Etat.

(3): Il s'agit d'une modification rédactionnelle.

(5): Voir sous article 4 (3).

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 pertinentes 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 pénale.

~~(2) Le recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique compétente en la matière.~~

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

~~(3) Les données relatives aux jugements civils ou administratifs, de même que les sanctions administratives sont traitées sous le contrôle de l'autorité publique compétente en la matière.~~

(4) Quiconque effectue un traitement en violation des dispositions du présent ~~de cet~~ 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 fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.

Commentaires:

La commission propose un réagencement des paragraphes. Le paragraphe (3) devient un paragraphe (1). En effet, ce paragraphe concerne les procédures judiciaires dans son ensemble, alors que les paragraphes (2) et (3) (après réagencement) ne se réfèrent qu'aux procédures répressives ou aux résultats de celles-ci.

(1): Cette disposition vise à permettre aux autorités judiciaires, sur la base d'une disposition légale expresse, d'effectuer des traitements de données en relation avec des enquêtes ou procédures judiciaires en cours. Plutôt que de réglementer ce type de traitement dans la présente loi, il paraît préférable d'effectuer un renvoi au droit commun en matière de procédure (pénale, civile ou administrative).

La formulation de ce paragraphe du présent article est suffisamment contraignante pour indiquer que le juge ne saurait procéder à des traitements en dehors de tout mécanisme de contrôle. Il s'agira toutefois d'un contrôle interne qui est seul admissible dans la logique de la séparation des pouvoirs. Il s'exercera au titre des règles procédurales de droit commun, notamment du Code d'instruction criminelle. La formulation est suffisamment ouverte pour permettre d'introduire, à l'avenir, des modifications dans le Code d'instruction criminelle, si des problèmes devaient surgir que les mécanismes existants ne permettraient pas de résoudre.

(3): Reprise du texte du Conseil d'Etat.

(4): Voir sous article 4 (3).

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

(1) Sans préjudice des dispositions prévues dans la législation sur la liberté dans les moyens de communication de masse et dans la mesure où il s'avère nécessaire pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression, le traitement mis en oeuvre aux seules fins de journalisme ou d'expression artistique ou littéraire n'est pas soumis:

(a) lorsque le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou à des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée:
   – 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;

(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~~s~~ (1) ~~et (2)~~, lorsque leur application compromettrait la collecte des données auprès de la personne concernée et
   – de l'article 26 paragraphe (~~3~~ 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;

(d) au droit d'accès de la personne concernée qui peut être différé ou limité conformément à l'article 28 paragraphe (4) et à l'article 29.

(2) Lors de la notification d'un traitement effectué à des fins de journalisme ou d'expression artistique ou littéraire, la notification ne renseigne que sur le(s) nom(s) et adresse(s) du responsable du traitement ou de son représentant.

(3) La Commission nationale, conformément aux pouvoirs qui lui sont conférés par la présente loi et dans le respect des règles relatives à la liberté d'expression, ne peut opérer qu'en présence du président de l'organe représentatif de la presse ou de son délégué, dès lors qu'un traitement visé au paragraphe (1) est impliqué.

Commentaires:

Cet article transpose l'article 9 de la directive 95/46 qui ne laisse aucune latitude aux Etats membres en la matière. C'est la raison pour laquelle la commission a décidé de maintenir l'article 9 ainsi que les dispositions se référant à cet article 9.

L'article 9 s'applique aux traitements mis en œuvre aux seules fins de journalisme ou d'expression artistique ou littéraire. La future loi sur la liberté dans les moyens de communication de masse va prévoir des dispositions particulières uniquement en cas de traitement mis en œuvre aux fins de journalisme.

(1) (c): Les amendements tiennent compte de la fusion des paragraphes (1) et (2) de l'article 26 en un seul paragraphe (1).

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 ~~exprès~~, 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 ~~qu'il~~ que le lieu en question présente ~~dans sa situation~~ 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 ~~, à la prévention, la recherche, la constatation et la poursuite d'infractions pénales~~, ou

~~(c) dans une résidence privée dont le responsable du traitement est la personne physique y domiciliée.~~

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

(2) ~~Sans préjudice du droit à l'information prévu à l'article 26, les~~ 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 oeuvre 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 (3).

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

(a) si la personne concernée a donné son consentement ~~exprès~~ sauf le cas interdit par la loi ~~nonobstant des dispositions contraires de 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 devant lesquelles exercer ou défendre un droit en justice.

~~(4) Le traitement à des fins de surveillance exclusivement mis en oeuvre pour la prévention des infractions pénales est soumis à l'obligation d'information excluant ainsi application de l'article 27 paragraphe (1) (d).~~

(~~5~~ 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 fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du paragraphe (1) du présent article.

Commentaires:

(1) (b): Rejet de la proposition du Conseil d'Etat de restreindre les lieux visés aux seuls lieux accessibles au public. Le but du projet de loi est de ne pas créer de distinction artificielle entre le lieu accessible au public et celui qui ne l'est pas. La commission a cependant exclu les locaux d'habitation. Pour le reste, la commission a repris la proposition de texte du Conseil d'Etat visant à inclure la prévention des accidents et à omettre la prévention, la recherche, la constatation et la poursuite d'infractions pénales.

(1) (c): Reprise du texte du Conseil d'Etat. En ce qui concerne les personnes morales, doivent être visés non seulement le siège social, mais aussi le siège des succursales et des établissements.

(2): Reprise de la proposition du Conseil d'Etat d'ajouter à la fin du paragraphe (2) une référence au paragraphe (1) (b). La commission estime nécessaire d'y inclure aussi une référence à la lettre (c). Elle supprime la référence à l'article 26 figurant au début du paragraphe et ajoute la possibilité pour la personne concernée de demander les informations visées à l'article 26 (3). Il est en effet irréaliste de penser que l'information préalable ou concomitante prévu au paragraphe (2) de l'article 10 puisse inclure toutes les informations prescrites à l'article 26 (3).

(3): Reprise du texte du Conseil d'Etat

(4): Reprise de la proposition du Conseil d'Etat de supprimer le paragraphe (4).

(4) nouveau: voir sous article 4 (3).

Art. 11. – ***Traitement à des fins de surveillance sur le lieu du travail***

(1) Le traitement à des fins de surveillance sur le lieu de travail peut être mis en oeuvre, conformément à l'article 14, par l'employeur s'il en est le responsable. Un tel traitement n'est possible que s'il est nécessaire:

(a) pour les besoins de sécurité et de santé des travailleurs, ou

(b) pour les besoins de protection des biens de l'entreprise, ou

(c) pour le contrôle du processus de production portant uniquement sur les machines, ou

(d) pour le contrôle temporaire de production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte, ou

(e) dans le cadre d'une organisation de travail selon l'horaire mobile conformément à la loi.

Dans les cas visés aux lettres (a), (d) et (e), le comité mixte d'entreprise, le cas échéant institué, a un pouvoir de décision tel que défini à l'article 7 paragraphes (1) et (2) de la loi modifiée du 6 mai 1974 instituant des comités mixtes dans les entreprises du secteur privé et organisant la représentation des salariés dans les sociétés anonymes. Le consentement ~~exprès~~ de la personne concernée ne rend pas légitime le traitement mis en oeuvre par l'employeur.

(2) Sans préjudice du droit à l'information de la personne concernée ~~celle-ci ainsi que le comité mixte ou à défaut la délégation du personnel ou à défaut encore l'Inspection du Travail et des Mines sont informés par l'employeur~~ 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.

(3) Quiconque effectue un traitement en violation des ~~contrevient aux~~ dispositions du présent article est puni d'une peine d'emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros

~~10.001 à 5.000.000 LUF~~, ou d'une des peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.

Commentaire:

Ce texte a été proposé par la commission du travail et de l'emploi. La commission s'est ralliée à cette proposition. Il est renvoyé au document parlementaire 4735[7] pour le commentaire.

(3): Voir sous article 4 (3).

Chapitre III. – ***Formalités préalables à la mise en œuvre des traitements et publicités des traitements*** ~~***Notification et publicité des traitements***~~

Art. 12. – ***Notification préalable à la Commission nationale***

~~Obligation de notification à la Commission~~

~~(1) Préalablement à la mise en œuvre d'un traitement ou d'un ensemble de traitements ayant une même finalité ou des finalités liées, le responsable du traitement, ou son représentant, la notifie à la Commission.~~

(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.

(2) Pour les traitements des données dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ainsi qu'aux droits et libertés des personnes concernées, la Commission nationale établit et publie des normes en vue d'une notification simplifiée.

Ces normes précisent:

a) la ou les finalités du traitement faisant l'objet d'une notification simplifiée;

b) la ou les catégories de données traitées;

c) la ou les catégories de personnes concernées;

d) les destinataires ou catégories de destinataires auxquels les données sont communiquées;

e) la durée de conservation.

Les traitements qui correspondent à ces normes font l'objet d'une notification simplifiée de conformité envoyée à la Commission nationale le cas échéant par voie électronique.

~~(2)~~ (3) Est exempté de l'obligation de notification:

(a) le responsable du traitement qui désigne un chargé de la protection des données tenu notamment d'assurer, de manière indépendante, l'application des dispositions légales en la matière et d'établir et de continuer à la Commission nationale un registre des traitements effectués par le responsable du traitement conformément aux dispositions relatives à la publicité des traitements telles que prévues à l'article 15;

(b) le traitement ayant pour seul objet 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) le traitement soumis à l'autorisation par voie réglementaire prévue à l'article 17;~~

(c) ~~(d)~~ le traitement mis en œuvre conformément aux règles de procédures judiciaires en matière civile et nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice.

(4) ~~(3)~~ Quiconque ne se soumet pas à l'obligation de notification ~~telle que prévue au paragraphe (1) qui précède~~ ou fournit des informations incomplètes ou inexactes est puni d'une amende de 251 à

125.000 euros. ~~10.001 à 1.000.000 LUF.~~ La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.

~~(4) Quiconque fournit lors de la notification sciemment des informations incomplètes ou inexactes est puni d'un emprisonnement de huit jours à six mois et d'une amende de 10.001 à 3.000.000 LUF, ou d'une de ces peines seulement.~~

Commentaires:

(1) (a): Cet amendement a pour objet de simplifier la procédure initialement proposée en précisant qu'à l'exception des traitements expressément soumis aux dispositions prévues aux articles 8, 14 et 17, tous les autres traitements de données à caractère personnel font l'objet d'une notification préalable. La référence au représentant du responsable du traitement a été biffée, dans la mesure où ce représentant, prévu uniquement lorsque le responsable du traitement n'est pas domicilié au sein de l'Union européenne (article 3 (2) alinéa 2), se substitue au responsable du traitement dans l'accomplissement des obligations incombant à celui-ci en vertu de la présente loi à venir. Partant toute référence au responsable du traitement implique et inclut nécessairement le représentant de ce responsable.

(1) (b): L'ajout d'un point (b) répond au souci du déclenchement d'une avalanche de notifications et détermine les cas dans lesquels une notification unique est possible.

(2): L'ajout d'un paragraphe (2) relatif à l'introduction d'une notification simplifiée répond au même souci susénoncé. La notification simplifiée tend à alléger la procédure de notification afin d'éviter que la Commission nationale ne soit submergée dès le départ par une vague d'informations énorme difficile à traiter. Cette proposition d'amendement s'inspire du projet de loi français intitulé „protection des personnes physiques à l'égard des traitements de données à caractère personnel" (No 3250; www.assemblée.nationale.fr).

(3) (a): La commission est d'avis que le chargé de la protection des données doit, puisqu'il n'y a pas de notification préalable, continuer son registre des traitements à la Commission nationale afin de mettre celle-ci en mesure de remplir sa mission de surveillance.

(3) (c): La lettre (c) est supprimée. La référence à l'article 17 a été insérée au paragraphe (1) lettre (a). La lettre (d) devient partant la lettre (c). La référence à la „matière civile" vise à exclure les procédures judiciaires répressives visées à l'article 8.

(4): Voir sous article 4 (3). Reprise de la proposition du Conseil d'Etat.

Art. 13. – ***Contenu et forme de la notification***

(1) La notification comprend au moins les informations suivantes:

(a) le nom et l'adresse du responsable du traitement, et le cas échéant de son représentant et du sous-traitant;

(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;

(h) la durée de conservation des données.

(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.

(3) La notification se fait auprès de la Commission nationale moyennant support papier ou informatique suivant un schéma à établir par elle. Il est accusé réception de la notification.

~~(4) Quiconque contrevient aux dispositions des paragraphes (1) et (2) qui précèdent est puni d'une amende de 10.001 à 1.000.000 LUF.~~

(4) ~~(5)~~ Un règlement grand-ducal fixera le montant et les modalités de paiement d'une redevance à percevoir lors de toute notification et de toute modification de notification.

Commentaires:

(1) (b): Il s'agit d'introduire une information supplémentaire quant au respect de la condition de légitimité du traitement (article 5).

(4): Reprise de la proposition du Conseil d'Etat de supprimer le paragraphe (4).

Art. 14. – ***Autorisation préalable de la Commission nationale***

(1) Sont soumis à l'autorisation préalable de la Commission nationale:

(a) les traitements prévus aux articles 6 paragraphe (2) a), b), e), g), 6 paragraphe (4) b), ~~11 et le cas échéant ceux prévus à~~ aux articles ~~l'article~~ 7 (1), ~~et~~ 10 et 11 de la présente loi;

(b) les traitements de données à des fins historiques, statistiques ou scientifiques visés à l'article 4 paragraphe (2). La Commission nationale vérifie en particulier si ces traitements ne peuvent être réalisés sur base de données rendues anonymes;

(c) l'interconnexion de données à caractère personnel visée à l'article 16;

(d) le traitement concernant le crédit et la solvabilité des personnes concernées;

(e) l'utilisation de données ~~à caractère personnel~~ 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.

~~(2) L'autorisation n'est délivrée par la Commission qu'après examen préalable à la mise en oeuvre des traitements visés au paragraphe (1). L'examen préalable est effectué dès la réception de la notification.~~

~~L'autorisation à délivrer en matière de traitement à des fins de surveillance sur le lieu de travail est subordonnée à l'avis préalable de l'Inspection du Travail et des Mines.~~

(2) La demande d'autorisation comprend au moins les informations suivantes:

(a) le nom et l'adresse du responsable du traitement ou de son représentant et le cas échéant du sous-traitant;

(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 aux articles 22 et 23;

(j) la durée de conservation des données.

(3 ~~b~~) 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.

(4 ~~3~~) Quiconque effectue un traitement en violation des dispositions du présent ~~de cet~~ article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 7.500 euros ~~de 10.001 à 5.000.000 LUF~~, ou d'une de ces peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.

Commentaires:

(1) (a): Les traitements visés à l'article 10 (traitements à des fins de surveillance) doivent faire l'objet d'une autorisation préalable par la Commission nationale.

(1) (d): Maintien du texte d'origine au motif que les notions critiquées par le Conseil d'Etat peuvent être rapprochées de l'ébranlement du crédit et de la cessation des payements déjà connues en droit commercial.

(1) (e): Cette précision fait suite aux „plus vives appréhensions" exprimées par le Conseil d'Etat.

(2): Ce nouveau paragraphe précise le contenu minimal d'une demande d'autorisation. Le parallèle avec l'article 13 (1) est évident. Cependant, les dispositions des lettres (e) et (f) ainsi que de la lettre (i) sont plus restrictives qu'à l'article 13 (1) lettres (d) et (g) respectivement.

(3): L'amendement a pour objet d'éviter des demandes surabondantes en cas de traitements qui ont une même finalité, qui portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires. Dans ces cas, la Commission nationale peut prendre une décision unique d'autorisation.

(4): Voir sous article 4 (3).

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 13, paragraphe (1); et

(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 (3) (a).

(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) (f) et à l'article 14, paragraphe (2) (i).

(5) Cependant la Commission nationale peut limiter l'accès ou différer l'exercice du droit d'accès lorsqu'une telle mesure est nécessaire pour sauvegarder:

(a) la sûreté de l'Etat,

(b) la défense,

(c) la sécurité publique,

(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 de procédures judiciaires autres, au sens de l'article 8, paragraphe 3, et de l'article 17 de la présente loi,

(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.

Commentaires:

(1) à (3): Ces paragraphes indiquent les informations devant figurer sur le registre public des traitements.

(4) et (5): Ces dispositions gouvernent l'accès à ce registre. L'accès est gratuit. Le registre est en ligne. Toutefois la Commission nationale peut limiter l'accès ou en différer l'exercice dans des cas limitativement énumérés et identiques à ceux relatifs au droit d'information et d'accès (articles 27 et 28). L'exception tirée du secret professionnel n'est pas mentionnée aux articles 27 et 28, dans la mesure où, contrairement aux hypothèses qui y sont visées, l'accès au registre est ouvert au public.

(5) (b): il est renvoyé au commentaire de l'article 3 (3).

(6): Il s'agit du paragraphe (4) du texte initial. La proposition du Conseil d'Etat sur l'état des notifications et autorisations est inscrite à l'article 32 (2), qui est jugé plus approprié par la commission.

(7): Il s'agit du paragraphe (5) du texte initial

Art. 16. – ***Interconnexion de données ~~à caractère personnel~~***

(1) L'interconnexion de données ~~à caractère personnel~~ qui n'est pas expressément prévue par un texte légal doit faire l'objet d'une autorisation préalable de la Commission nationale sur demande conjointe présentée ~~demandée~~ par les responsables des traitements en cause ~~conjointement~~.

(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.

(3) L'interconnexion n'est autorisée que dans le respect des finalités identiques ou liées de fichiers et du secret professionnel.

~~(3) Un règlement grand-ducal peut déterminer les modalités de mise en oeuvre des traitements visés au paragraphe (1).~~

Commentaires:

(1): Reprise du texte du Conseil d'Etat. Il est simplement précisé que l'autorisation dont question est une autorisation préalable.

(2): Maintien du texte initial.

(3): L'interconnexion n'est possible que si les finalités des différents traitements de données sont soit identiques soit liées. Il appartient à la Commission nationale de vérifier leur compatibilité et de n'autoriser l'interconnexion que si les finalités des différents traitements de données sont compatibles

entre elles. Il appartient également à la Commission nationale de veiller dans ce contexte au respect du régime du secret professionnel auquel sont soumises certaines professions. La référence au règlement grand-ducal jugée inappropriée par le Conseil d'Etat a été supprimée.

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, à la constatation et à la poursuite 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 police et de l'administration des douanes et accises f~~ont l'objet d'un règlement grand-ducal. Leur responsable est le Procureur d'Etat territorialement compétent~~ . Le règlement grand-ducal déterminera ~~notamment le Procureur d'Etat~~ 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, et

(b) les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique ~~font l'objet d'un 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 à caractère personnel 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 ci-dessus.

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, qui inclut l'accès informatique, aux données traitées 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 intéressée 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 fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.

Commentaires:

(2): Au regard du caractère sensible des données visées à cet article, le contrôle et la surveillance des traitements de celles-ci sont opérés par une autorité ad hoc composée de le Procureur Général d'Etat ou de son délégué, qui la préside et de deux membres de la Commission nationale.

(3): Le texte initial pourrait, en effet, être interprété en ce sens que les forces de l'ordre sont exposées à des sanctions pénales, si elles agissent en dehors du cadre réglementaire. La sanction pénale devra, à l'évidence, être limitée aux personnes agissant à titre particulier, la surveillance des forces de l'ordre

étant assurée par l'autorité de contrôle et les activités des agents relevant du contrôle interne. Voir également sous article 4 (3).

Chapitre IV. – *Transferts de données vers des pays tiers*

Art. 18. – ***Principes***

(1) Le transfert vers un pays tiers de données ~~à caractère personnel~~ faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement après leur transfert ~~vers un Etat non membre de l'Union européenne~~, 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 ~~pour la protection des données~~ qui apprécie si un pays tiers assure un niveau de protection adéquat. La Commission nationale ~~pour la protection des données~~ 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 ~~pour la Protection des Données~~ 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 ~~10.001 à 5.000.000 LUF,~~ ou d'une de ces peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions des paragraphes (1), (2) et (4) du présent article.

Commentaires:

(1): Reprise du texte du Conseil d'Etat avec utilisation de la définition de „données" figurant à l'article 2 (e).

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 ~~exprès~~ 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 vie~~ de la personne concernée, ou

(f) le transfert intervienne depuis un registre public tel que prévu à l'article 12, paragraphe (2) lettre (b).

(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 notifier à la Commission nationale un rapport établissant les conditions dans 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 ~~à caractère personnel~~ vers un pays tiers ~~un Etat non membre de l'Union européenne~~ 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 ~~des paragraphes (2) et (3)~~ est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ~~10.001 à 5.000.000 LUF,~~ ou d'une de ces peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.

Commentaires:

(1) (e): Reprise du texte du Conseil d'Etat.

(3): Reprise du texte du Conseil d'Etat.

Art. 20. – *Information réciproque*

(1) La Commission nationale ~~pour la protection des données~~ informe le ministre ~~compétent en la matière~~ de toute décision prise en application de l'article 18, paragraphes (3) et (4) et de l'article 19 paragraphes (1) et (2). Le ministre en informe la Commission européenne.

(2) Le ministre ~~compétent en la matière~~ informe la Commission nationale de toute décision relative au niveau de protection d'un pays tiers ~~Etat non membre de l'Union européenne~~ prise par la Commission européenne.

Commentaire:

Reprise des propositions du Conseil d'Etat et mise en conformité de la désignation du ministre avec la définition portée à l'article 2 (k).

Chapitre V. – *~~Confidentialité~~ Subordination et sécurité des traitements*

Art. 21. – *~~Confidentialité des traitements~~ 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.

Commentaire:

Reprise de la proposition du Conseil d'Etat. Le titre de l'article 21 et partant du chapitre V lorsqu'il se réfère à la „confidentialité" semble inapproprié. La commission a décidé de lui substituer „Subordination".

Art. 22. – *Sécurité des traitements*

(1) Le responsable du traitement doit mettre en œuvre toutes les mesures techniques et d'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. Ces mesures font l'objet d'un ~~examen~~ rapport annuel à soumettre par le responsable du traitement à la Commission nationale. ~~dont le résultat est communiqué à la Commission~~

(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

(b) les obligations visées au présent article incombent également à celui-ci.

~~(4) Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures visées au présent article sont consignés par écrit.~~

Commentaires:

(1) et (2): Reprise du texte du Conseil d'Etat

(3): Rejet de l'appréciation du Conseil d'Etat selon laquelle le paragraphe (3) serait superflu. La précision de l'expression „consignation par écrit" étant une exigence de forme qui justifie l'utilité de sa présence dans ce paragraphe.

(4): Reprise de la proposition du Conseil d'Etat de supprimer le paragraphe (4)

Art. 23. – ***Mesures de sécurité particulières***

En fonction ~~Compte ten~~u 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).

Commentaire:

La modification a été proposée par le Conseil d'Etat.

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 ~~c~~Code pénal, même après la fin de leur mandat.

(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. ~~modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93 du 13 décembre 1999 relative à un cadre communautaire pour les signatures électroniques, la directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE du 20 mai 1997 concernant la vente à distance des biens et des services autres que les services financiers.~~

(4) Le responsable du traitement agissant dans le cadre de l'accomplissement de ses missions ~~tel que~~ visées à l'article 7, paragraphe (1), 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), (5) et (6).

Commentaires:

(1): Rejet de la proposition du Conseil d'Etat de supprimer la mention „même après la fin de leur mandat". Il ne s'agit non seulement de fonctionnaires ou des personnes jouissant d'un statut assimilé mais le cas échéant de personnes externes. C'est la raison pour laquelle ce rappel d'une règle de droit commun est important.

(3): Reprise du texte du Conseil d'Etat.

(4): La proposition de texte du Conseil d'Etat n'a pas été retenue. Il s'agit en fait de l'application du droit commun de l'article 458 du Code pénal selon lequel le titulaire du secret professionnel, dont le fondement est la protection de la vie privée de la personne concernée, ne peut lui opposer ce secret. Conformément à l'avis du Conseil d'Etat, il y a lieu d'encadrer l'accès aux données relatives à la santé. Toutefois cet encadrement ne peut consister en une limitation des types de renseignements accessibles. La protection de la vie privée de la personne concernée se limite à la seule hypothèse dans laquelle la Commission nationale agirait de son propre chef. Dès lors qu'elle est saisie sur requête de la personne concernée rien ne s'oppose à ce que la Commission nationale ait accès aux données de la requérante.

Art. 25. – ***Sanctions relatives à la ~~confidentialité~~ 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 ~~10.001 à 3.000.000 LUF~~, ou d'une de ces peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions des articles 21, 22 et 23.

Commentaire:

L'intitulé de cet article a été modifié pour tenir compte de la modification de l'intitulé de l'article 21.

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 ~~ou son représentant~~ 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;
– la durée de conservation des données.

~~(2) Lorsque la collecte des données se fait moyennant formulaire ou questionnaire, quel que soit son support ou moyennant des documents qui servent de base à la collecte des données, ils doivent contenir les informations visées au paragraphe (1).~~

(2~~3~~) Lorsque les données n'ont pas été collectées auprès de la personne concernée, le responsable du traitement ~~ou son représentant~~ doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée, 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;
– la durée de conservation des données.

(3 ~~4~~) Quiconque contrevient aux dispositions du présent article ~~de cet article~~ est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ~~10.001 à 5.000.000 LUF~~, ou d'une de ces peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.

Commentaires:

(1): Reprise de la proposition du Conseil d'Etat dont le contenu est intégré au paragraphe (1).

La commission a repris la proposition du Conseil d'Etat de supprimer le paragraphe (2). Les paragraphes suivants sont donc renumérotés en conséquence.

(1) et (2): En ce qui concerne la suppression de la référence au représentant: voir sous article 12 (1) (a).

(1) (b) et (2) (b): l'ajout de l'adjectif „déterminées" vise à éviter que le responsable du traitement n'indique que des finalités vagues, ce qui serait préjudiciable à l'information de la personne concernée.

(3): Voir sous article 4 (3).

Art. 27. – ***Exceptions au droit à l'information de la personne concernée***

(1) L'article 26, paragraphes (1) et (2 3) ne s'applique pas lorsque le traitement est nécessaire pour sauvegarder:

(a) la sûreté de l'Etat;
(b) la défense;
(c) la sécurité publique;
(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 de procédures judiciaires autres, au sens de l'article 8, paragraphe 3, et de l'article 17 de la présente loi ~~ou de manquements à la déontologie dans le cas des professions réglementées~~;
(e) un intérêt économique ou financier important de l'Etat ou de l'Union européenne, ~~en particulier~~ y compris dans les domaines monétaire, budgétaire et fiscal;

(f) la protection de la personne concernée ou des droits et libertés d'autrui,

(2) Les dispositions de l'article 26 sont susceptibles de dérogations lors de la collecte de données dans les conditions prévues à l'article 9 paragraphe (1) (c).

(3) Les dispositions de l'article 26 paragraphes (1) et (2 ~~3~~) 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 ~~10.001 à 5.000.000 LUF~~, ou d'une de ces peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions des paragraphes (1) et (2) du présent article.

Commentaires:

(1) et (3): Il s'agit d'une rectification suite à la renumérotation de l'article 26.

(1) (b): Il est renvoyé au commentaire de l'article 3 (3).

(1) (d): L'amendement (d) a pour but de restreindre le droit d'information en cas de traitement nécessaire à la prévention, la recherche, la constatation et la poursuite d'infractions pénales y compris celles à la lutte contre le blanchiment, ou au déroulement de procédures judiciaires autres, au sens de l'article 8, paragraphe 3, et de l'article 17 de la présente loi. La même exception se retrouve aux articles 15 et 29 (1) (d).

(1) (e): Reprise de la proposition du Conseil d'Etat

(2): Rejet de la proposition du Conseil d'Etat de supprimer ce paragraphe, dans la mesure où l'article 9 est maintenu.

(4): Voir sous article 4 (3)

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 condition de prouver son/leur identité, la personne concernée, ou ses ayants droit justifiant d'un intérêt légitime, peu(ven)t obtenir à sa/leur demande auprès du responsable du traitement, ou de son représentant sans contrainte, 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 paragraphe (1).

(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 ~~10.001 à 5.000.000 LUF~~, ou d'une de ces peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.

(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 et à la demande de son curateur ou de son tuteur.

~~et collectées par son médecin. Le droit d'accès peut être exercé par le patient lui-même ou par l'intermédiaire d'un médecin qu'il désigne. En cas d'incapacité de la personne concernée, le droit d'accès peut être exercé par ses ayants droit.~~

(4) Toute personne a un droit d'accès aux données la concernant et utilisées aux fins d'un traitement mis en oeuvre dans le cadre de la liberté d'expression tel que prévu à l'article 9. Aussi longtemps que les données auxquelles l'accès est demandé n'ont pas été publiées, la communication de ces données, ainsi que toute information disponible sur leur origine ne peut se faire que par l'intermédiaire de la Commission nationale qui opère conformément à l'article 9, paragraphe (3) de la présente loi.

(5) Selon le cas, le responsable du traitement ~~ou son représentant~~ 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.

(6) 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.

(7) Toute rectification, tout effacement ou verrouillage effectué conformément au paragraphe (5) sera notifié sans délai par le responsable du traitement ~~ou son représentant~~ aux destinataires auxquels les données ont été communiquées, à moins que cela ne s'avère impossible.

(8) Sans préjudice de la sanction prévue au paragraphe (5), quiconque contrevient sciemment aux dispositions du présent article ~~de cet 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 ~~10.001 à 5.000.000 LUF~~, ou d'une de ces peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.

Commentaires:

(1): Reprise du texte du Conseil d'Etat sauf que la référence au représentant du responsable du traitement a été supprimée (voir sur ce point: article 12 (1) (a)).

(1), (5) et (7): Quant à la suppression du représentant, il est renvoyé à l'article 26.

(2) et (8): Il s'agit d'une infraction nécessitant un dol général. La fermeture définitive ou temporaire a également été incluse.

(3): L'amendement du premier alinéa a pour objet de déterminer les ayants droit qui exercent le droit d'accès en cas d'incapacité de la personne concernée. Pour le cas du décès du patient l'amendement reprend le texte figurant à l'article 36 alinéa 5 de la loi du 28 août 1998 sur les établissements hospitaliers sous peine de créer un conflit de lois entre une loi spéciale (à application hospitalière) antérieure et une loi postérieure (celle relative à la protection des personnes à l'égard du traitement des données à caractère personnel) à application générale.

(4): Rejet de la proposition du Conseil d'Etat de supprimer ce paragraphe, dans la mesure où l'article 9 est maintenu.

(5): Reprise de la proposition du Conseil d'Etat avec adaptation à la nouvelle numérotation des articles suite à l'inversion des chapitres VII et VIII.

(5) et (7): La référence au représentant du responsable du traitement a été supprimée (voir: article 12 (1) (a)).

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;

(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 de procédures judiciaires autres, au sens de l'article 8, paragraphe 3, et de l'article 17 de la présente loi; ~~ou de manquements à la déontologie dans le cas des professions réglementées;~~

(e) un intérêt économique ou financier important de l'Etat ou de l'Union européenne, y compris ~~en particulier~~ 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 et que la mesure d'exception est prise conformément à l'article 28, paragraphe (4);

(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).

(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 ~~à caractère personnel~~ 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.

(3) 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.

(4) 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.

(5) Quiconque contrevient à la disposition du paragraphe (3) qui précède est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros, ~~10.001 à 5.000.000 LUF~~ ou d'une de ces peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du paragraphe (3) du présent article.

Commentaires:

(1) (b): Il est renvoyé à l'article 3 (3).

(1) (d): Il est renvoyé à l'article 27 (1) (d).

(3) et (4): Reprise du texte du Conseil d'Etat.

(5): voir sous article 4 (3).

Art. 30. – ***Droit d'opposition de la personne concernée***

(1) Toute personne concernée a le droit:

(a ~~1~~) 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 oeuvre par le responsable du traitement ne peut pas porter sur ces données;

(b ~~2~~) de s'opposer, sur demande et gratuitement, au traitement la concernant envisagé par le responsable du traitement 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 ~~3~~) 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, ~~10.001 à 3.000.000 LUF~~ ou d'une de ces peines seulement. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.

Commentaires:

Réagencement de l'article 30 conformément à la proposition du Conseil d'Etat.

(1) (b): Rejet de la proposition du Conseil d'Etat.

L'article 14 (b) de la directive 95/46/CE pose le principe et les conditions dans lesquelles le droit d'opposition joue en matière de prospection. Dans ce cadre, la notion de prospection peut recouvrir des significations plus variées que celle visée à l'article 48 de la loi du 14 août 2000 sur le commerce électronique. La prospection à but non commercial y est également couverte par l'article 30.

De plus, le commerce électronique conformément à l'article 1e paragraphe (5) point b) ainsi que le considérant 14 de la directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information est entièrement soumis aux dispositions législatives en matière de protection des données comprises dans les directives 95/46/CE et 97/66/CE et donc dans la législation en cours de transposition. Le champ d'application de la protection des données étant plus large que celui du commerce électronique.

Enfin, l'article 7 paragraphe (2) de la directive 2000/31/CE ne fait que définir les modalités d'une des deux formes possibles (à savoir l'opt-out) du droit d'opposition.

La définition des champs respectifs de ces deux formes (opt in/opt out) est faite par renvoi aux directives 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications et 97/7/CE concernant la vente à distance des biens et des services autres que les services financiers.

Dès lors, la transposition du principe fondateur du droit d'opposition compris à l'article 14 de la directive 95/46 et à l'article 30 du projet de loi ne saurait se satisfaire de l'article 48 de la loi sur le commerce électronique vu son champ d'application et son contenu.

(2): Voir sous article 28 (2) et 28 (8).

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:

(1) ~~Toute personne a le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité.~~

(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.

Commentaire:

(1): Reprise du texte du Conseil d'Etat étant donné qu'il s'agit d'un texte plus protecteur. On passe du principe selon lequel la décision individuelle automatisée est possible à celui d'une prohibition générale à l'exclusion des hypothèses a) et b).

Chapitre VII. – *Contrôle et surveillance de l'application de la loi*

Commentaire:

La commission a décidé de renverser l'ordre des chapitres VII et VIII. La logique veut que les recours devant les juridictions judiciaires soient décrites après que les missions de la Commission nationale aient été détaillées.

Art. 32 – *Missions et pouvoirs de la Commission ~~N~~nationale ~~pour la Protection des Données~~*

(1) Il est institué une autorité de contrôle dénommée „Commission nationale pour la protection des données“ „~~Commission Nationale pour la Protection des Données“ dénommée dans la présente loi „la Commission~~“, chargée de contrôler et de vérifier si les données ~~à caractère personnel~~ 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 oeuvre 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 oeuvre 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);

~~émettre un avis préalable à l'adoption des mesures réglementaires ou administratives et être consultée préalablement à l'adoption de tout texte de loi portant création d'un traitement, ainsi que de tout projet de modification de ces mesures ou texte de loi, l'avis est publié dans les documents parlementaires et dans le rapport de la Commission;~~

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

(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, ~~ou par une association la représentant~~, d'une demande relative au respect de ses droits et libertés fondamentaux à l'égard d'un traitement. La personne concernée est informée des suites réservées à sa requête.

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

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

(~~6~~ 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.

(~~7~~ 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.

(~~8~~ 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 ~~nécessaire à l'accomplissement de leurs missions respectives ou en exerçant ses pouvoirs sur demande d'une de celles-ci.~~

(~~9~~ 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. ~~de même qu'à toute autorité de contrôle commune instituée par des instruments juridiques internationaux.~~

(~~10~~ 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 ~~10.001 à 5.000.000 LUF~~, 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. La juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données avec les dispositions du présent article.

Commentaires:

Il s'agit de l'article 34 du texte initial.

(1): Reprise des propositions du Conseil d'Etat.

(2): La commission reprend la proposition du Conseil d'Etat faite à l'endroit de l'article 15 (4), à savoir que le rapport annuel de la Commission nationale doit également renseigner sur l'état des notifications. Elle inscrit cette proposition dans l'article 32 (2) qu'elle estime être l'endroit approprié.

S'agissant de l'avis requis de la commission consultative des droits de l'homme (CCDH), la commission s'exprime en principe en faveur de l'implication d'une commission consultative des droits de l'homme, dont l'instauration a été demandée par certains représentants des „forces vives de la nation" afin d'assurer une certaine surveillance de la Commission nationale et un regard critique sur les avis de la Commission nationale. La CCDH est un organe consultatif du Gouvernement en matière de droits de l'homme qui trouvera une base légale dans le présent article alors que son fonctionnement interne actuellement régi par l'arrêté ministériel du 26 mai 2000. Un représentant du domaine de la „protection des données" devrait à l'avenir être membre de la CCDH.

La Commission nationale est une autorité indépendante sous tutelle administrative. Ces deux qualificatifs ne sont pas incompatibles. En effet la loi prohibe toute ingérence de qui que ce soit dans la prise de décision ce qui n'empêche pas un contrôle de bonne gestion et de bonne administration.

(3) (e): Reprise du texte du Conseil d'Etat avec modification de la référence faite initialement à l'article 15 (4), suite à la nouvelle rédaction de cet article 15.

(4): Reprise du texte du Conseil d'Etat.

(5): Amendement en vue de répondre à la préoccupation du Conseil d'Etat face à une ouverture très large du droit de saisine.

(6): Ce nouveau paragraphe vise à imposer à la Commission nationale un délai d'un mois à compter de sa saisine pour se prononcer sur l'existence d'une violation de l'article 11. en cas de saisine en vertu des paragraphes (4) et (5), le délai de 3 mois inscrit dans la législation sur la procédure administrative non contentieuse s'applique. Cette différence de traitement s'explique par l'importance de faire cesser toute surveillance sur le lieu du travail qui contreviendrait aux dispositions de l'article 11.

(8) et (9): Les amendements font suite aux critiques du Conseil d'Etat.

(10): Reprise de la proposition du Conseil d'Etat.

(11): Reprise de la proposition du Conseil d'Etat. En ce qui concerne la limitation aux „locaux autres que d'habitation", il s'agit de faire un parallèle avec le paragraphe (7). Le terme „volontairement" a été remplacé par „sciemment" pour plus de cohérence avec les infractions visées aux articles 28 (2), 28 (8) et 30 (2). Le dol général est donc requis.

Art. 33. – ***Sanctions administratives***

~~Sans préjudice des poursuites pénales éventuelles et des peines d'emprisonnement et/ou des amendes prévues par la présente loi, le responsable du traitement, son représentant ou le cas échéant le sous-traitant dont les traitements sont soumis au contrôle de la Commission nationale, peuvent être frappés par celle-ci, après une procédure contradictoire, d'une amende d'ordre qui ne peut dépasser 10.000.000 francs lorsqu'il s'agit d'une personne morale et de 500.000 francs lorsqu'il s'agit d'une personne physique pour l'une des infractions commises à la présente loi et/ou à ses règlements d'exécution ainsi qu'aux instructions de la Commission nationale. En cas de récidive, le montant de l'amende d'ordre sera doublé.~~

(1 ~~2~~) La Commission nationale peut prendre les sanctions disciplinaires suivantes: ~~prononcer soit en sus de l'amende d'ordre l'une ou l'autre des 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 ~~condamnée~~;

(2 ~~3~~) 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. ~~Sanctions précitées seront prises dans le respect du principe du contradictoire et des droits de la défense. Un règlement grand-ducal peut déterminer les modalités de la procédure contradictoire".~~

Commentaires:

Il s'agit de l'article 35 du texte initial.

(1): Le paragraphe (1) reprend les propositions du Conseil d'Etat. La lettre (d) a été remaniée d'un point de vue formel en s'inspirant de l'article 39 (5).

(2): Reprise du texte du Conseil d'Etat.

La commission a également décidé de faire sienne la proposition du Conseil d'Etat de supprimer le paragraphe (3).

Art. 34. – ***Composition de la Commission ~~N~~nationale ~~pour la Protection des Données~~***

(1) La Commission nationale est une autorité publique ~~indépendante~~ qui prend la forme d'un établissement public ~~doté de la personnalité juridique, d'une autonomie administrative et financière~~. Son siège est fixé ~~établi~~ 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 ayant la protection des données dans ses attributions.

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. ~~Dont un président et un vice-président nommés par le Grand-Duc pour un terme de six ans renouvelable une fois.~~ Le président est désigné par le Grand-Duc. Les membres sont nommés pour un terme de six ans, renouvelable une fois.

Avant d'entrer en fonction, le président de la Commission nationale prête entre les mains du Grand-Duc 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."

(3) 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. ~~Grand-Duc nommera les membres sur proposition du Gouvernement en conseil. Le Gouvernement en conseil proposera comme membre effectif au moins un juriste et un informaticien justifiant d'une formation universitaire accomplie.~~

~~Les membres de la Commission nationale sont proposés pour leur compétence professionnelle reconnue dans leur(s) matière(s) respective(s).~~

(4) 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 ~~à caractère personnel~~.

(5) 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. ~~Leur mandat cesse de plein droit dès l'atteinte de la limite d'âge de soixante-cinq ans.~~

(6) Avant d'entrer en fonction, les membres de la Commission nationale prêtent entre les mains du président assermenté 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."

Commentaires:

(1): Reprise du texte du Conseil d'Etat. Il a cependant été précisé que le siège de la Commission nationale initialement fixé à Luxembourg-ville peut être transféré par règlement grand-ducal en toute autre localité du Luxembourg. En raison de cet ajout, le premier alinéa comprend 3 phrases au lieu d'une pour plus de clarté.

(2): La commission a remplacé le conseil du gouvernement par le gouvernement en conseil, estimant que cette dénomination est plus appropriée et est d'ailleurs déjà utilisée aux articles 32 (2) et 35 (7). En ce qui concerne la révocation des membres de la Commission nationale, il est renvoyé à l'article 35 (7).

La commission a repris la proposition du Conseil d'Etat de soumettre le président de la Commission nationale à la prestation de serment conformément à l'article 110 de la Constitution. Le serment du vice-président est réglé de la même manière que celui des autres membres de la Commission nationale.

(3): Le second alinéa a été supprimé comme proposé par le Conseil d'Etat. Pour le reste, le paragraphe (3) ne comprend qu'une fusion des 2 phrases composant précédemment le premier alinéa pour plus de clarté et afin d'éviter un double emploi avec le premier alinéa du paragraphe (2).

(5): La limite d'âge a été supprimée alors qu'elle est jugée inutile par la commission.

(6): Adaptation du texte suite à la remarque du Conseil d'Etat de soumettre le président de la Commission nationale à la prestation de serment.

Art. 35. – ***Fonctionnement de la Commission ~~N~~nationale ~~pour la Protection des Données~~***

(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 ~~B~~.

(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) les modalités de désignation du président et du vice-président,~~

(~~d~~ 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. ~~Que si la majorité de ses membres en exercice présents ou suppléés participe à la séance.~~

(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. ~~La Commission constate préalablement à chaque délibération les conflits d'intérêts opposables à ses membres et suspend leur droit de vote jusqu'à la délibération suivante.~~

(6) Les délibérations ~~de la Commission~~ sont prises à la majorité des voix. Les abstentions ne sont pas recevables. ~~Absolue des membres présents. Toutefois, sont prises, à la majorité d'au moins deux voix les délibérations suivantes:~~

~~(a) l'adoption et la modification du règlement intérieur;~~

~~(b) l'émission d'un avis ou l'octroi d'une autorisation.~~

(7) Le Gouvernement en conseil ayant proposé à la nomination un membre de la Commission nationale peut proposer sa révocation au Grand-Duc ~~après avis conforme de la Commission pris à la majorité des membres présents.~~ La Commission nationale est demandée 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.

Commentaires:

Il s'agit de l'article 37 du texte initial.

(1): Reprise de la proposition du Conseil d'Etat de supprimer la référence au Mémorial „B".

(2) (c): Reprise de la proposition du Conseil d'Etat.

(3) à (6): Reprise du texte du Conseil d'Etat.

Art. 36. – ***Statut des membres et agents de la Commission ~~N~~nationale ~~pour la Protection des Données~~***

(1) La Commission nationale est assistée dans l'exercice de ses missions par des agents nommés et placés sous son autorité.

(2) Les membres effectifs et agents de la Commission nationale sont des employés privés à assimiler à des employés de l'Etat, sans préjudice des dispositions de la présente loi et de celles d'un règlement grand-ducal à prendre en matière de cadre, de rémunération et de promotion des membres effectifs et des agents de la Commission nationale. Les indemnités des membres suppléants sont fixées par règlement grand-ducal.

(3) Avant d'entrer en fonctions les agents prêtent entre les mains du président assermenté de la Commission nationale le serment qui suit: „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."

(4) Les rémunérations et autres indemnités de tous membres, agents et employés de la Commission nationale sont à charge de la Commission nationale.

(5) Le cadre du personnel de la Commission nationale pourra être complété par des employés et des ouvriers, nécessaires au bon fonctionnement, dans les limites des crédits budgétaires de la Commission nationale.

(6) La Commission nationale peut, dans des cas déterminés, ~~également~~ faire appel à des experts externes dont les prestations sont définies et rémunérées ~~qui sont engagés~~ sur la base d'un contrat de droit privé.

Commentaires:

Il s'agit de l'article 38 du texte initial.

(2): Les amendements font suite aux remarques du Conseil d'Etat. Il y a donc une différenciation entre le régime applicable aux membres effectifs et aux membres suppléants de la Commission nationale.

(3): L'amendement vise à établir un parallèle avec l'article 34 (2) (anciennement article 36 (2)).

(6): Reprise du texte du Conseil d'Etat.

Art. 37. – ***Dispositions financières***

(1) Au moment de sa création, la Commission nationale ~~pour la protection des données~~ bénéficie d'une dotation initiale de deux cent mille ~~X millions~~ d'euros ~~de francs~~ à charge ~~à faire part~~ du budget de l'Etat ainsi que d'un apport de 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 ~~approuve son bilan~~ de l'exercice précédent, ensemble avec son rapport de gestion. Avant le 30 septembre de chaque exercice, la Commission nationale arrête ~~approuve~~ le budget pour l'exercice à venir. Le budget, les comptes annuels et les rapports arrêtés ~~approuvés~~ sont transmis au ~~Conseil de Gouvernement~~ 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.

(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 à l'article 13 de la présente loi. Pour le solde des frais restant à couvrir dans le cadre de ses missions conférées par la présente loi, la Commission nationale bénéficiera d'une dotation d'un montant à déterminer sur une base annuelle et à inscrire au ~~faire part du~~ budget de l'Etat.

(5) La loi du 27 novembre 2001 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2002 est modifié comme suit: il est ajouté au budget des dépenses au Chapitre III – Dépenses courantes sous „00 – Ministère d'Etat" une section „00.9 Commission nationale pour la protection des données" émargeant les articles suivants:

„12.300: Prise en charge par l'Etat des frais encourus par la Commission nationale pour la protection des données. (crédit non limitatif et sans distinction d'exercice) … 200.870

33.000: Dotation initiale en faveur de la Commission nationale pour la protection des données … 200.000"

Commentaires:

Il s'agit de l'article 39 du texte initial.

(1): Reprise des propositions du Conseil d'Etat.

(3): Reprise des propositions du Conseil d'Etat. Pour ce qui est de l'utilisation du „Gouvernement en conseil" plutôt que du „Conseil de Gouvernement", il est renvoyé à l'article 34 (2).

(4): Reprise de la proposition du Conseil d'Etat avec la précision que la dotation annuelle pour couvrir le solde des frais vise les missions conférées à la Commission nationale par la loi à venir.

(5): L'amendement a pour objet de modifier la loi du 27 novembre 2001 concernant le budget des dépenses et des recettes de l'Etat pour l'exercice 2002 aux fins d'y inclure dans le chapitre III du budget des dépenses sous 00 – Ministère d'Etat une section 00.9 en vue de la prise en charge des frais encourus par la Commission nationale (art.12.300) et la dotation initiale octroyée à celle-ci (art.33.000)

Chapitre VIII. – *Recours juridictionnels*

Commentaire:

L'intitulé du chapitre VIII fait abstraction d'une référence à la „responsabilité" et précise qu'il s'agit d'un recours juridictionnel, car un recours auprès de la Commission nationale est déjà prévu à l'article 32.

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.

Commentaire:

Il peut être fait abstraction d'une référence au recours devant la Commission nationale, car, d'une part, ce recours a déjà été explicité et, d'autre part, le présent chapitre ne vise que les recours juridictionnels.

Le recours visé à l'article 33 (actuellement 35), paragraphe 2, n'a pas besoin d'être visé, puisqu'il ne vise pas un recours mis en œuvre par la personne „victime" d'un traitement contraire aux prescriptions

du présent projet de loi. C'est la raison pour laquelle une référence a été faite aux actions pénales qui peuvent être intentées par cette même personne.

Pour une meilleure lisibilité, le début du paragraphe (1) de l'article suivant a été intégré à l'article 38.

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'établis- sement 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 d'acquittement irrévocable par le juge pénal.

Commentaires:

Il s'agit de remplacer le recours devant la chambre du conseil par une action calquée sur l'action en cessation prévue à l'article 21 de la loi du 27 novembre 1986 réglementant certaines pratiques commerciales et sanctionnant la concurrence déloyale.

Le paragraphe (2) s'inspire de la jurisprudence rendue en application de la loi du 27 novembre 1986 précitée (Cour 19 octobre 1977, Pas.24, 46, Cour 31 mai 1978, Pas.24, 127).

La suspension provisoire intimement liée à la cessation est obligatoire en cas de violation de la loi. La fermeture provisoire n'est que facultative.

Il est opportun de prévoir une sanction contre le sous-traitant, même si ce dernier, au vœu de l'article 21, ne peut procéder à un traitement que sur ordre du responsable du traitement.

Se pose encore la question de savoir si la fermeture provisoire de l'établissement du sous-traitant pourra être ordonnée même si ce sous-traitant effectue des traitements pour des responsables de traitement autres que le responsable contrevenant. D'après le texte reproduit ci-dessus la fermeture provisoire pourra être ordonnée même en pareille hypothèse. Certes le sous-traitant agit sous les ordres du responsable du traitement, mais il a une obligation de veiller à la légalité du traitement et devra s'opposer à des instructions du responsable du traitement, lorsqu'il estime que ces instructions débouchent sur un traitement contrevenant aux dispositions de la loi.

Chapitre IX. – *Le chargé de la protection des données*

Commentaire:

La commission a inséré l'article 40 dans un chapitre séparé. Il était en effet assez curieux de faire figurer le chargé de la protection des données dans le chapitre relatif à la Commission nationale.

Art. 40. – ***Le chargé de la protection des données***

(1) Tout responsable de traitement peut, dans le cadre de l'article 12, paragraphe (3 ~~2~~) sous (a), et aux fins y visées, désigner un chargé de la protection des données, dont il communique l'identité à la Commission nationale.

~~(2) Les missions du chargé de la protection des données sont les suivantes:~~

~~(a) assurer l'application des dispositions de la présente loi et de ses règlements d'exécution aux traitements qu'il est appelé à surveiller;~~

~~(b) tenir un registre des traitements effectués par le responsable du traitement identique à celui tenu par la Commission nationale quant à son contenu et son fonctionnement afin de garantir que ces traitements ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées.~~

(2 3) 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.

(3 ~~4~~) 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:

(a) il ne connaît aucun lien de subordination vis-à-vis du responsable du traitement et ne peut être lié au responsable du traitement par un contrat de travail:

~~(b) il ne peut subir de désavantage du fait de l'exécution de ses missions;~~

(b c) il ne peut être révoqué pour des raisons liées à l'exercice de ses missions, hormis le cas de la violation de ses obligations légales ~~et/~~ou conventionnelles.

(4 ~~5~~) Le chargé de la protection 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.

(5 ~~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. ~~, ou celles pouvant exercer cette activité de plein droit.~~

(6 ~~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 ainsi que d'assises financières d'une valeur de 20.000 euros ~~quinze millions de francs au moins. L'agrément est délivré par la commission nationale~~

(7 ~~8~~) Par dérogation au paragraphe précédent, les membres inscrits dans une des professions réglementées suivantes peuvent ~~immédiatement exercer l'activité de~~ 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.

(8 9) La Commission nationale vérifie les qualités de tout chargé de la protection des données. ~~Qu'il soit agréé ou membre d'une des professions réglementées visées au paragraphe qui précède, en exami-~~

~~nant son activité professionnelle antérieure à la désignation, et en organisant un contrôle continu et/ou en l'examinant sur sa connaissance de la matière.~~

Elle ~~La Commission~~ 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 à caractère personnel 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.

(9 ~~10~~) La Commission définit les modalités du contrôle continu des qualités requises à la fonction de chargé de la protection des données ~~en organisant des formations à valider~~.

(10 ~~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.

Commentaires:

(1): Reprise du texte du Conseil d'Etat. La référence au paragraphe (2) de l'article 12 a été remplacée par celle au paragraphe (3) de ce même article en raison de la renumérotation intervenue suite à l'ajout à cet article 12 d'un nouveau paragraphe (2).

(2): Suppression du paragraphe (2) initial comme préconisé par le Conseil d'Etat et renumérotation des paragraphes suivants.

(3) (b): Suppression de la lettre (b), alors que le chargé de la protection des données ne peut être salarié du responsable du traitement (lettre (a)). Ainsi la lettre (b) initiale devient superflue: étant indépendant du responsable du traitement, le chargé de la protection des données ne peut subir de désavantage du fait de ses missions.

(3) (b) (nouveau): Reprise de la proposition du Conseil d'Etat.

(5) à (7): Le paragraphe (5) établit l'exigence d'un agrément pour pouvoir exercer les fonctions de chargé de la protection des données. Les conditions qu'un candidat doit remplir, à savoir qualification professionnelle et assises financières, sont prévues au paragraphe (6). La dernière phrase de ce paragraphe (6) a été supprimée du fait d'une redondance avec le paragraphe (5). Les assises financières ont été ramenées à 20.000 €. Les membres de certaines professions réglementées peuvent être agréés sans autre condition que leur appartenance à ces professions réglementées. Parmi les avocats, seuls les avocats à la Cour peuvent être agrées. La commission s'est inspirée du projet de loi 4790 portant, entre autres, transposition de la directive 98/5/CE du Parlement européen et du Conseil du 16 février 1998 visant à faciliter l'exercice permanent de la profession d'avocat dans un Etat membre autre que celui où la qualification a été acquise. L'article 15 de ce projet de loi tend à modifier la loi du 31 mai 1999 régissant la domiciliation des sociétés en ce sens que seuls les avocats à la Cour peuvent être domiciliataires.

(8): Reprise de la proposition du Conseil d'Etat. Ajout de la possibilité pour la Commission nationale de s'opposer à la désignation et au maintien d'un chargé de la protection des données.

(9): Suppression de la référence aux „formations à valider". La formation continue doit se concevoir de manière plus large.

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) ~~et le procureur d'Etat agissant en matière de flagrant crime~~ 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 (ci-après „ILR") aux données concernant l'identité des abonnés et utilisateurs des opérateurs et fournisseurs de ~~télé~~communications électroniques ainsi que des services postaux et des fournisseurs de ces services. ~~A ces fins, les opérateurs et les fournisseurs mettent d'office et gratuitement à la disposition de l'ILR les données relatives aux abonnés, utilisateurs et leurs services.~~

La centrale des secours d'urgence 112 accède 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). ~~relatives à l'identité des abonnés et utilisateurs, et à leurs services.~~ Les données doivent être ~~mises à jour~~ 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 ~~télé~~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.

(3 ~~2~~) 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, ~~ainsi que~~ celles prises en matière de ~~flagrant délit~~ 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 .

(4 ~~3~~) La procédure est entièrement automatisée suite à l'autorisation de la Commission nationale. La Commission nationale vérifiera en particulier la sécurisation du système informatique utilisé. Cette automatisation permettra l'accès à distance par voie de communication électronique.

~~Si une requête est introduite dans le cadre des mesures spéciales de surveillance telles que prévues aux articles 88-1 à 88-4 du Code d'instruction criminelle, ainsi que dans le cadre des mesures prises en matière de flagrant délit, l'ILR l'exécute dans un délai de 24 heures dès sa réception. Si une requête est introduite en vue de l'accomplissement d'une mission de sauvegarde de la vie humaine, l'ILR l'exécute immédiatement dès réception de celle-ci. Un ou plusieurs fonctionnaires de l'ILR, désignés à des fins, sont chargés de l'exécution des requêtes après des opérateurs et/ou de leurs fournisseurs de services prévus à l'article 41 paragraphe (1).~~

Commentaires:

(1): L'amendement a pour objet de répondre aux inquiétudes exprimées par le Conseil d'Etat. L'accès a été limité aux autorités agissant dans le cadre des articles 88-1 à 88-4 du code d'instruction criminelle, dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du code d'instruction criminelle. La commission a également ajouté la centrale des secours d'urgence 112 .

Ces autorités et centrale n'ont accès qu'aux données relatives à l'identité des abonnés et utilisateurs, à savoir nom, prénoms, adresse et, le cas échéant, l'adresse IP.

La centrale des secours d'urgence 112 n'a pas accès aux données des services postaux. La commission ne voit en effet pas l'utilité d'accès à ces données étant entendu que seule une situation d'urgence justifie une demande d'accès émanant de ladite centrale.

(2): Il s'agit de la deuxième phrase du paragraphe (1) qui a été reprise dans un nouveau paragraphe (2) pour plus de lisibilité. Cette phrase a été modifiée pour tenir compte de la nouvelle rédaction du paragraphe (1). La suppression de „et à leurs services" sert à rendre le texte plus lisible. En outre il appartient au règlement grand-ducal de déterminer les services en question. La commission a également procédé à quelques modifications purement textuelles.

(3): Reprise de la proposition de texte du Conseil d'Etat avec adaptation compte tenu de la rédaction du paragraphe (1).

(4): Reprise de l'idée avancée par le Conseil d'Etat. Il est précisé que la procédure est entièrement automatisée. Cette précision s'avère, après vérification avec ILR, indispensable du fait qu'un traitement „manuel" d'une requête soumise par fax ou lettre présuppose

1) du côté de l'ILR la mise en place d'un dispositif supplémentaire en matière de ressources humaines, et
2) crée un problème de responsabilité dans le chef de l'ILR du fait que celui-ci serait amené à apprécier l'origine et l'exactitude de ces requêtes ce qui n'est pas son rôle. L'esprit de l'article 41 est d'offrir un outil technique destiné à avoir plus facilement accès au nom de la personne et à son numéro de téléphone (IP adresse …) nonobstant les procédures déclenchées préalablement. L'ILR n'est qu'un interface entre opérateurs et données.

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).

Commentaire:

Rejet de la proposition du Conseil d'Etat d'ajouter un paragraphe (4). La préoccupation exprimée par le Conseil d'Etat est répercutée à l'article 44.

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 ~~trois~~ 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. ~~Dans ce cas, le délai prévu au paragraphe (2) qui précède est de rigueur.~~

(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).

Commentaires:

(1): La commission a jugé un délai de 4 mois plus approprié.

(3): La suppression de la dernière phrase s'explique par le fait que les responsables du traitement se verront découragés d'avancer la notification ou la demande d'autorisation avant la fin de la période de validité de l'autorisation octroyée à ce jour.

Art. 44. – *Dispositions finales*

(1) La loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, ~~telle qu'elle a été modifiée par les lois des 19 novembre 1987, 30 septembre 1992, 1er octobre 1992 et 9 août 1993~~ 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.

Commentaires:

(1): Reprise de la proposition du Conseil d'Etat.

(2): Cet amendement a pour objet de combler le vide juridique qui résulterait d'une abrogation expresse des règlements grand-ducaux pris en exécution de la loi modifiée du 31 mars 1979 citée ci-contre. Cette formule permet aux anciens règlements d'exécution, trouvant une base légale suffisante dans le nouveau texte, de rester en vigueur jusqu'à ce qu'il est pourvu à leur remplacement par de nouvelles dispositions.

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.

Commentaire:

La commission a jugé plus réaliste une entrée en vigueur différée comme le suggère le Conseil d'Etat. Cependant, afin de permettre la mise en place de la Commission nationale le plus rapidement possible, il est prévu que les dispositions régissant l'organisation de celle-ci entrent en vigueur trois jours après publication de la loi au Mémorial.

*

Au nom de la Commission précitée je vous saurais gré de bien vouloir m'envoyer dans les meilleurs délais l'avis du Conseil d'Etat sur les amendements exposés ci-dessus.

Copie de la présente est envoyée pour information au Premier Ministre, Ministre d'Etat, au Ministre délégué aux Communications et au Ministre aux Relations avec le Parlement.

Veuillez agréer, Monsieur le Président, l'expression de ma considération très distinguée.

Jean SPAUTZ
Président de la Chambre des Députés

Service Central des Imprimés de l'Etat

4735/10

N° 4735[10]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

AVIS COMPLEMENTAIRE DU CONSEIL D'ETAT

(2.7.2002)

Sur la base de l'article 19(2) de sa loi organique du 12 juillet 1996 le Conseil d'Etat fut saisi le 6 juin 2002 par le Président de la Chambre des Députés d'une série d'amendements au projet de loi sous rubrique, adoptés par la commission des Médias et des Communications au cours de sa réunion du 5 juin 2002.

Les modifications proposées, accompagnées de leur commentaire, étaient intégrées dans une nouvelle version coordonnée du projet de loi en discussion.

*

Le Conseil d'Etat note avec satisfaction que bon nombre des suggestions et propositions consignées dans son avis du 29 janvier 2002 sur le projet de loi sous examen *(Doc. parl. No 4735[6], sess. ord. 2001-2002)* trouvent leur reflet dans le texte entériné par la commission parlementaire compétente. Sont notamment à mentionner à cet égard les amendements en rapport avec les articles 32 à 36 concernant la Commission nationale pour la protection des données et ceux ayant trait à l'article 41 réglementant l'accès à certaines données relatives aux abonnés et services offerts par les opérateurs et fournisseurs de communications électroniques ou postales.

Dans ce contexte le Conseil d'Etat salue plus particulièrement l'abandon, par les auteurs des amendements, des **sanctions administratives** initialement prévues à l'article 35. Dans son avis précité il avait en effet vivement critiqué l'institution d'amendes d'ordre à côté de sanctions pénales, en raison notamment du fait que cette juxtaposition risquerait de causer, le cas échéant, problème au regard du principe fondamental du „non bis in idem".

De sérieuses réserves sont par contre de mise au regard du réagencement des **sanctions pénales** figurant aux articles 4 (3) – qualité des données, 5 (2) – légitimité du traitement, 6 (5) – traitement de catégories particulières, 7 (5) – traitement de catégories particulières de données par les services de la santé, 8 (4) – traitement de données judiciaires, 10 (4) – traitement à des fins de surveillance, 11 (3) – traitement à des fins de surveillance sur le lieu de travail, 12 (4) – notification préalable à la Commission nationale, 14(4) – autorisation préalable de la Commission nationale, 17 (3) – autorisation par voie réglementaire, 18 (5) – principes (en matière de transfert de données vers des pays tiers), 19 (4) – dérogations (dans le même domaine), 25 – sanctions relatives à la subordination et à la sécurité des traitements, 26 (3) – le droit à l'information de la personne concernée, 27 (4) – exceptions au droit à l'information de la personne concernée, 28 (2) et (8) – droit d'accès, 29 (5) – exceptions au droit d'accès, 30 (2) – droit d'opposition de la personne concernée, 32 (11) – missions et pouvoirs de la Commission nationale et 41 – dispositions spécifiques. Tous ces articles prévoient en effet qu'en dehors des peines d'emprisonnement et d'amende à sa disposition, „la juridiction saisie peut prononcer la fermeture de l'établissement de manière définitive ou jusqu'à la mise en conformité du traitement des données (avec les prescriptions violées)".

De par sa vocation d'application générale à des acteurs divers, agissant dans un contexte hétéroclite, cette nouvelle peine accessoire introduite par les auteurs des amendements sous revue ne peut être maintenue telle quelle et mérite pour le moins d'être nuancée.

Il n'est en effet guère concevable d'ordonner la fermeture d'une entreprise ayant, en violation des prescriptions de l'article 11, opéré un traitement à des fins de surveillance sur le lieu de travail. Ou encore d'envisager la même sanction dans le chef d'un établissement hospitalier qui aurait mis en oeuvre le traitement de données particulièrement sensibles sans observer les règles prescrites par l'article 7. Pourrait-on d'ailleurs frapper de la même peine les autorités impliquées dans une enquête pénale ou encore les organes du corps de la police grand-ducale, de l'Inspection générale de la police et de l'administration des douanes et accises au titre d'*établissements* ayant procédé sans respecter respectivement les dispositions prévues aux articles 8 et 17? Ces quelques exemples devraient à suffisance illustrer les carences du système.

Force est de relever que l'approche adoptée dans le cadre du nouvel article 39 instituant une action en cessation est autrement pertinente.

Aussi le Conseil d'Etat propose-t-il en ordre principal d'abandonner la peine accessoire de la fermeture définitive ou provisoire et de la remplacer par l'ordre de cessation – sous peine d'astreinte – du traitement contraire aux dispositions légales. Toujours dans la même approche une autre solution de rechange pourrait consister dans l'ordre de faire détruire – aux frais de la personne condamnée – toute donnée recueillie ou traitée en violation de la loi. En ordre subsidiaire le Conseil d'Etat estime que la sanction de la fermeture ne pourrait être maintenue que dans le contexte d'hypothèses très particulières à définir et encore qu'à l'égard d'établissements dont la seule activité est de traiter des données à caractère personnel.

*

Dans l'examen du texte des amendements le Conseil d'Etat se concentrera sur quelques modifications essentielles en rapport avec les articles 1er (objet), 2 (définitions), 3 (champ d'application), 7 (traitement de catégories particulières de données par les services de la santé), 8 (traitement de données judiciaires), 9 (traitement réalisé dans le cadre de la liberté d'expression), 10 (traitement à des fins de surveillance), 11 (traitement à des fins de surveillance sur le lieu du travail), 12 (notification préalable à la Commission nationale), 14 (autorisation préalable de la Commission nationale), 15 (publicité des traitements), 16 (interconnexion de données), 17 (autorisation par voie réglementaire), 19 (dérogations à la solution de principe régissant les transferts de données vers des pays tiers), 22 (sécurité des traitements), 24 (secret professionnel), 27 (exceptions au droit à l'information de la personne concernée), 28 (droit d'accès), 29 (exceptions au droit d'accès), 32 (missions et pouvoirs de la Commission nationale), 34 (composition de la Commission nationale), 35 (fonctionnement de la Commission nationale), 36 (statut des membres et agents de la Commission nationale), 37 (dispositions financières), 39 (action en cessation), et 44 (dispositions finales) de la nouvelle version du projet de loi sous revue.

Article 1er

Comme le Conseil d'Etat a eu l'occasion de le relever dans son avis du 29 janvier 2002 sur le projet de loi sous examen, l'article 1er se propose d'étendre la protection aux personnes morales en étalant de la sorte son champ d'application au-delà des domaines visés par la directive 95/46 CE et la Convention de Strasbourg qui restent limités aux personnes physiques. Le projet de loi s'attelait plus spécialement à faire „respecter les intérêts légalement protégés des personnes morales", étant entendu que selon son commentaire „la référence à l'intérêt légalement protégé (…) permet de prévenir l'utilisation de certains droits tirés de la présente loi à des fins illégitimes". Dans son avis susmentionné le Conseil d'Etat avait estimé que la référence à la légitimité des intérêts d'une personne morale serait autrement pertinente que la mention de ses intérêts légalement protégés et avait proposé une reformulation de texte en conséquence. Il n'a pas été suivi sur ce point par les auteurs des amendements sous revue au motif que „ „la protection légale de la personne morale" est une expression plus restrictive que celle d'„intérêt légitime" utilisée dans la directive". Cet argument est pour le moins insolite, alors que la directive précisément laisse les personnes morales en dehors de ses visées!

Article 2

Le Conseil d'Etat approuve la démarche des auteurs des amendements sous avis de présenter dans l'ordre alphabétique les définitions essentielles du texte légal en élaboration, alors que le projet initial les présentait dans l'ordre de leur apparition dans le dispositif normatif. La nouvelle approche est en effet de nature à faciliter la recherche et mérite partant d'être retenue.

En elles-mêmes les définitions amendées se recouvrent largement avec celles proposées par le Conseil d'Etat dans son avis du 29 janvier 2002. Pour la plupart elles ne commandent donc plus d'observation, sauf quant à celles déterminant l'instance médicale et le fichier de données à caractère personnel.

La motivation de l'amendement en rapport avec la lettre (i) – antérieurement (g) – consistant à mentionner spécialement parmi les instances médicales „tout établissement hospitalier visé par la loi du 28 août 1998 sur les établissements hospitaliers" ne semble pas très convaincante. En effet le Conseil d'Etat n'entrevoit pas de quelle manière la redéfinition de l'instance médicale couvrirait dorénavant les organismes tels que la Croix-Rouge ou encore la Ligue luxembourgeoise de Prévention et d'action médico-sociales, mentionnées au commentaire de la disposition en cause et qu'il s'agirait précisément d'y inclure.

La reformulation de la notion de fichier de données à caractère personnel sous la lettre (h) – (d) au projet originaire – se doit d'être évoquée en raison de son caractère incisif. Au vœu de l'amendement proposé les ensembles non structurés de données échappent désormais à la protection assurée par la loi en perspective. La nouvelle définition, si elle se recoupe avec la notion telle que déterminée à l'article 2c) de la directive, aurait mérité d'être plus solidement argumentée au regard surtout des motifs à la base du texte initial retenant que la „définition, plus large que celle prévue dans la directive, permet d'éviter de donner l'impression qu'on ne protège que les données reprises dans les „fichiers informatiques classiques" mais qu'elle inclut toutes les formes de données possibles (ex. formes structurées: système de gestion de bases de données qui attribuent une signification très précise à chaque donnée (colonne d'une table), forme moins structurée: dans les logiciels de traitement de texte qui permettent de gérer des données (dans les tableaux), forme non structurée: dans les logiciels de traitement de texte)". La justification du revirement opéré paraît en tout cas quelque peu confuse et n'est pas très concluante.

Article 3

Au paragraphe (2), alinéa 1, sous la lettre (b) le premier tiret avec son texte subséquent peut être biffé alors que par définition le responsable du traitement établi sur le territoire luxembourgeois est soumis au droit luxembourgeois et, en tant que tel, range dans la catégorie visée sous la lettre (a) du même paragraphe. Il en découle que la disposition en cause se lira comme suit:

> „*(b) le traitement mis en oeuvre 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 le territoire d'un autre Etat membre de l'Union européenne.*"

L'alinéa 2 du même paragraphe (2) est à introduire par la préposition „*pour*" en remplacement de „*par*".

Au paragraphe (5) le texte amendé précise sous le deuxième tiret que la loi ne s'applique pas „au traitement de données concernant une personne morale et dont la publication est prescrite par une loi ou un règlement". D'après le commentaire il s'agit en l'occurrence de données mises à la disposition du public du fait de leur publication au Mémorial. Le Conseil d'Etat en conclut que par exemple le traitement de données en relation avec le registre du commerce échapperait ainsi aux prescriptions de la future loi.

Article 7

L'article 6, paragraphe (1) interdit en principe „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".

L'article 7 énonce dans son paragraphe (1) une exception à cette règle générale en autorisant le traitement de données de l'espèce lorsqu'il est 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, (ainsi que) de la recherche scientifique dans le domaine de la biologie et de la médecine". A l'origine cette dérogation ne pouvait jouer qu'en faveur des instances médicales ainsi que des organismes de sécurité sociale et les administrations appelés à gérer cette catégorie particulière de données en exécution de leurs missions légales et réglementaires et pour autant qu'ils étaient soumis au secret professionnel.

Dans son avis du 29 janvier 2002 le Conseil d'Etat s'était interrogé s'il ne conviendrait pas d'y ajouter les entreprises d'assurance et les sociétés gérant les fonds de pension ou encore *certaines* mutuelles.

Les auteurs des amendements sous revue suivent le Conseil d'Etat dans sa suggestion tout en parlant cependant des mutuelles en général et en visant en outre „toute personne physique ou morale 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 oeuvrant dans les domaines social, familial et thérapeutique". Le Conseil d'Etat se prononce contre cette dernière extension en faveur des „ASFT" du pouvoir de traiter des données aussi sensibles. En l'absence de justification au commentaire de l'amendement en cause il a d'ailleurs du mal à en percevoir la nécessité alors que les risques d'abus ou de dérapage lui paraissent au contraire bien réels.

Le Conseil d'Etat n'est pas non plus favorable à l'inclusion dans les prévisions du paragraphe (1) de l'article 7 *des* mutuelles, au sens générique. Il n'est en effet guère recommandable d'étendre cette solution dérogatoire au principe ancré à l'article 6, à l'ensemble des caisses de décès, par exemple. L'on peut par contre très légitimement l'envisager dans le chef de la Caisse médico-chirurgicale mutualiste.

Le paragraphe (1) de l'article 7 mérite partant d'être revu en conséquence. Du point de vue formel, il y a lieu de remplacer dans la cinquième ligne par une virgule le point-virgule inséré entre le mot „médecine" et les termes „le traitement".

Article 8

Au paragraphe (1) l'adjectif „pertinentes" peut être biffé sans regret.

Au paragraphe (2) reprenant le texte de l'ancien paragraphe (1) il y a lieu d'écrire „disposition *légale*" au lieu de „disposition pénale".

Au paragraphe (4) il convient, par analogie à l'article 17, paragraphe (3), d'intercaler entre les mots „quiconque" et „effectue" l'incidente „agissant à titre privé" de sorte à le faire débuter comme suit:

„(4) quiconque, agissant à titre privé, effectue un traitement en violation …"

Article 9

Cet article est censé mettre en oeuvre l'article 9 de la directive 95/46/CE qui enjoint aux Etats membres de prévoir „pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations … dans la mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression". Au sens du texte communautaire les exemptions et dérogations, pour être légitimes, doivent être justifiées par la nécessité de concilier deux libertés et droits fondamentaux: liberté d'expression et droit à la vie privée. Ce n'est donc que dans l'intérêt de ce compromis nécessaire que les règles prévues aux Chapitres II (conditions générales de licéité des traitements à caractère personnel), IV (transfert de données à caractère personnel vers des pays tiers) et VI (autorité de contrôle et groupe de protection des personnes à l'égard du traitement des données à caractère personnel) peuvent être tenues en échec.

D'après le projet de loi sous revue (dans une version cependant légèrement restructurée par le Conseil d'Etat) ledit article 9 de la directive est appelé à se traduire en droit interne de la façon suivante:

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

(1) Sans préjudice des dispositions prévues dans la législation sur la liberté dans les moyens de communication de masse et dans la mesure où il s'avère nécessaire pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression, le traitement mis en oeuvre 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;

lorsque le traitement se rapporte à des données manifestement rendues publiques par la personne concernée ou à des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée;

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 de 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 la mise à disposition du public, de quelque manière que ce soit, de ces donnés ou fournirait des indications permettant d'identifier les sources d'information

e) au droit d'accès de la personne concernée qui peut être différé ou limité conformément à l'article 28 paragraphe (4) et à l'article 29.

(2) Lors de la notification d'un traitement effectué à des fins de journalisme ou d'expression artistique ou littéraire, la notification ne renseigne que sur le(s) nom(s) et adresse(s) du responsable du traitement ou de son représentant.

(3) La Commission nationale, conformément aux pouvoirs qui lui sont conférés par la présente loi et dans le respect des règles relatives à la liberté d'expression, ne peut opérer qu'en présence du président de l'organe représentatif de la presse ou de son délégué, dès lors qu'un traitement visé au paragraphe (1) est impliqué."

Le texte en question est quelque peu équivoque alors qu'il laisse entendre que les exceptions aux règles générales prévalant en la matière sont susceptibles de jouer dès que le *traitement* mis en oeuvre aux seules fins de journalisme ou d'expression artistique ou littéraire s'avère nécessaire pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression. Cette perspective paraît évidemment incompatible avec la philosophie à la base de l'article 9 de la directive 95/46 CE.

Aussi le Conseil d'Etat propose-t-il de remplacer dans la première phrase du paragraphe (1) les termes „il s'avère nécessaire" par ceux de „*où les dérogations ci-après s'avèrent nécessaires*".

Au vœu du paragraphe (3) la Commission nationale ne peut, dans le cadre des traitements y visés, agir „qu'en présence du président de l'organe représentatif de la presse ou de son délégué". Comment légitimer ce pouvoir exorbitant accordé aux organes de la presse? Que faire si ces derniers refusaient de collaborer avec la Commission nationale? La commission serait-elle en l'occurrence condamnée à l'inaction?

Face à ces incertitudes, le Conseil d'Etat serait plutôt favorable à l'élimination dudit paragraphe (3) de l'article 9.

De façon générale il reste par ailleurs attaché à sa préférence de ne pas préjuger de la réforme en perspective de la loi sur la presse et de reporter dans ce contexte la mise en oeuvre des obligations découlant de l'article 9 de la directive 95/46 CE.

Article 10

L'ajout des termes „autres que les locaux d'habitation" par les auteurs de l'amendement visé sous la lettre (b) du paragraphe (1) ne se justifie pas au regard de la nouvelle version du texte retenu sous la lettre (c) qui en évoquant les lieux d'accès privé les inclut nécessairement. Il peut partant en être éliminé.

Au paragraphe (3) le Conseil d'Etat propose de libeller comme suit la disposition figurant sous la lettre (c):

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

Il convient en effet de lever toute ambiguïté en la matière en précisant que les données collectées à des fins de surveillance peuvent être communiquées à toutes les autorités judiciaires et pas seulement aux autorités pénales.

Article 11

Le texte en question concerne le traitement à des fins de surveillance sur le lieu du travail et a été amendé à la lumière du rapport pour avis de la commission du Travail et de l'Emploi de la Chambre des députés du 15 mai 2002 *(Doc. parl. No 4735[7], sess. ord. 2001-2002)*. Le Conseil d'Etat en conclut qu'il tient compte des critiques formulées dans son avis du 29 janvier 2002 pour s'appliquer désormais et au secteur public et au secteur privé.

Article 12

Au regard du paragraphe (2) deux observations s'imposent.

Par référence à l'article 1er tel qu'amendé conformément à l'avis du Conseil d'Etat sur le projet de loi sous examen, il y a lieu d'écrire „dont la mise en oeuvre n'est pas susceptible de porter atteinte *aux libertés et droits fondamentaux, et notamment à la vie privée*, des personnes concernées", plutôt que „dont la mise en oeuvre n'est pas susceptible de porter atteinte à la vie privée ainsi qu'aux droits et libertés des personnes concernées". Il convient en outre de remplacer systématiquement à travers ledit paragraphe (2) le mot „normes" par celui de „directives" afin de ne pas laisser entrevoir que la Commission nationale disposerait en la matière d'un pouvoir réglementaire au sens propre du terme.

Article 14

Dans le contexte des traitements soumis à l'autorisation préalable de la Commission nationale le Conseil d'Etat donne à considérer s'il ne faut pas ajouter sous le paragraphe (1) lettre (a) les traitements visés à l'article 6, paragraphe (2) sous la lettre d) en rapport avec certaines données gérées par „une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale".

Dans la phrase introductive du paragraphe (2) il est proposé de radier l'expression „au moins".

Quant au paragraphe (4) le Conseil d'Etat note que sans un mot d'explication le plafond de l'amende pénale initialement fixé à 5.000.000 Luf a été réduit à 7.500 euros pour ne correspondre désormais plus qu'à quelque 302.550 francs!

Article 15

Au paragraphe (2) il y a lieu de substituer sous la lettre (b) la référence à l'article 14 à celle mentionnant l'article 13.

Dans le cadre du paragraphe (4) la mention de l'article 13, paragraphe (1) (g) doit remplacer celle renvoyant à l'article 13, paragraphe (1) (f).

Dans le contexte du paragraphe (5) le Conseil d'Etat préférerait écrire „cependant la Commission nationale peut limiter cette publicité lorsqu'une telle mesure est nécessaire pour sauvegarder …", afin d'éviter toute confusion avec la notion du droit d'accès de la personne concernée, visée aux articles 28 et 29. Compte tenu de la reformulation de l'article 8 il convient de corriger au même paragraphe (5) la référence à l'article 8, paragraphe (3) en celle de *„article 8, paragraphe (1)"*.

Article 16

En rapport avec l'amendement portant sur le paragraphe (3) le commentaire explique, entre autres, qu'„il appartient également à la Commission nationale de veiller dans ce contexte au respect du régime du secret professionnel auquel sont soumises *certaines* professions". Afin de mieux traduire cette nuance le Conseil d'Etat suggère de reformuler comme suit ledit paragraphe (3):

„L'interconnexion n'est autorisée que dans le respect des finalités identiques ou liées de fichiers et du secret professionnel *auquel les responsables du traitement sont le cas échéant astreints.*"

Article 17

Au paragraphe (1) il convient d'omettre sous la lettre (a) les termes „et à la poursuite des infractions pénales" de sorte que la disposition en question s'introduirait par le bout de phrase suivant:

„(a) les traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions pénales …"

Cette proposition est dictée par le souci d'opérer une séparation nette entre les traitements visés à l'article 17 et ceux relevant de l'article 8 dans le champ d'application duquel tombent précisément les actes de poursuite.

Au paragraphe (1) il est encore proposé d'ajouter sous une *lettre (c)* la disposition suivante garantissant une base légale aux traitements de données opérés dans le cadre de conventions internationales:

„(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)."

Au paragraphe (2), alinéa 6 il y a lieu d'écrire „Elle présente chaque année au ministre un rapport …".

A l'endroit de l'alinéa final du même paragraphe (2) il convient de faire remarquer que le droit d'accès de l'autorité de contrôle comporte nécessairement l'accès informatique, inutile de le préciser dans le texte même. Toujours dans le même contexte il se recommande d'employer le participe passé du verbe viser au lieu de celui de traiter.

Il s'en dégage que la phrase introductive dudit alinéa 7 doit s'énoncer comme suit:

„Le droit d'accès aux données visées au présent article ne peut être exercé que par l'intermédiaire de l'autorité de contrôle."

Article 19

Dans ce contexte il s'agit de redresser une erreur de référence au paragraphe (1), lettre (f) en y remplaçant la mention de l'article 12, paragraphe (2), lettre (b) par celle de l'article 12, *paragraphe (3)*, lettre (b).

Article 22

L'ajout par amendement de la conjonction de coordination „et" sous le paragraphe (3), lettre (a) ne peut être maintenu qu'à condition d'y adjoindre le mot „que" pour former ainsi la locution conjonctive „et que" enchaînant avec la disposition reprise sous la lettre (b).

Article 24

Au regard du paragraphe (1) le Conseil d'Etat maintient le point de vue exprimé dans son avis du 29 janvier 2002 selon lequel le bout de phrase „même après la fin de leur mandat" est à éliminer. En ordre subsidiaire il propose de substituer au terme „mandat" la notion plus neutre de „fonction" ou „mission" traduisant mieux le statut indépendant des membres et collaborateurs de la Commission nationale ainsi que du chargé de la protection des données.

Conformément au paragraphe (4) tel qu'amendé „le responsable du traitement agissant dans le cadre de l'accomplissement de ses missions visées à l'article 7, paragraphe (1), 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), (5) et (6)".

Rappelons que le responsable du traitement se meut en l'espèce dans le contexte de données très sensibles énoncées à l'article 6. Le délier en ces matières de son secret professionnel – et ne serait-ce qu'à l'égard de la seule Commission nationale – ne doit s'effectuer qu'avec prudence et circonspection.

Le Conseil d'Etat admet que cette condition est en principe remplie lorsque la Commission nationale est saisie par une personne d'une demande relative au respect de ses droits et libertés fondamentaux à l'égard d'un traitement ou encore dans le cadre 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, hypothèses visées à l'article 32, paragraphes (4) et (5). Il nourrit par contre de sérieuses réserves à l'égard du troisième cas mentionné au paragraphe (4) de l'article 24 qui serait susceptible de tenir en échec le respect du secret professionnel, savoir celui évoqué à l'article 32, paragraphe (6).

D'après le texte critiqué le secret professionnel ne pourrait ainsi être opposé à la Commission nationale saisie par l'une des personnes ou organes visés à l'article 11, paragraphe (2) concernant le traitement à des fins de surveillance sur le lieu de travail. Il s'agit en l'occurrence de la personne concernée, hypothèse ne soulevant quant à elle guère de problème, mais également, le cas échéant, du comité mixte, de la délégation du personnel, de l'inspection du travail et des mines et des organismes de représentation du personnel.

Le Conseil d'Etat estime que les auteurs de l'amendement sont ici allés trop loin et propose partant de rayer au paragraphe (4) de l'article 24 le renvoi au paragraphe (6) de l'article 32 et de s'en tenir à l'évocation de „l'article 32, paragraphes (4) *et* (5)".

Article 27

Au paragraphe (1) il y a lieu de corriger une erreur de renvoi sous la lettre (d) en mentionnant l'article 8, *paragraphe (1)*, et non pas l'article 8, paragraphe (3). Ce redressement s'impose compte tenu de la restructuration par amendement dudit article 8.

Article 28

Dans le cadre du paragraphe (1), lettre (d), la référence au paragraphe (1) de l'article 31 est à biffer, compte tenu de la version amendée de ce dernier.

Conformément au paragraphe (2) „celui qui entrave *sciemment* par quelque moyen que ce soit, l'exercice du droit d'accès" est passible de sanctions pénales. D'après son commentaire il s'agit d'une infraction nécessitant un dol général, à l'instar d'ailleurs de celle visée au paragraphe (8). La même solution se retrouve aux articles 30, paragraphe (2) et 32, paragraphe (11). Le Conseil d'Etat s'exprime en faveur de l'abandon de cette condition d'incrimination dans le cadre des dispositions en cause.

Il n'est en réalité pas convaincu par l'argumentation à la base dudit amendement alors que l'ajout de l'adverbe „sciemment" peut au contraire induire en erreur. Il est en effet discutable que l'emploi dudit terme fût à lui seul de nature à distinguer le caractère matériel ou non matériel de l'infraction et à la différencier ainsi par rapport à d'autres incriminations visées au projet.

Le paragraphe (3) reprend en ses deux premiers alinéas quasi textuellement les dispositions de l'article 36, alinéas 4 et 5 de la loi du 28 août 1998 sur les établissements hospitaliers. Le Conseil d'Etat approuve cette démarche des auteurs de l'amendement sous examen.

A l'endroit de l'alinéa 3 du même paragraphe (3), par souci de parallélisme avec les dispositions précédentes, le Conseil d'Etat propose une légère modification rédactionnelle en suggérant d'écrire *in fine* „par l'intermédiaire d'un médecin *désigné par* son curateur ou tuteur".

Article 29

Pour les raisons ci-avant développées à l'endroit de l'article 27 au paragraphe (1), lettre (d) il y a lieu d'invoquer comme référence *l'article 8, paragraphe (1).*

Article 32

Selon l'alinéa 2 du paragraphe (2), introduit par voie d'amendement, „le rapport (de la Commission nationale) 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".

Cette innovation est motivée comme suit d'après le commentaire dudit amendement:

> „S'agissant de l'avis requis de la commission consultative des droits de l'homme (CCDH), la commission (parlementaire) s'exprime en principe en faveur de l'implication d'une commission consultative des droits de l'homme, dont l'instauration a été demandée par certains représentants des „forces vives de la nation" afin d'assurer une *certaine surveillance* de la Commission nationale et un *regard critique* sur les avis de la Commission nationale …"

Le Conseil d'Etat n'est pas convaincu du bien-fondé de cette mesure. Conformément à l'article 34, paragraphe (1), alinéa final la Commission nationale „exerce en toute indépendance les missions dont elle est investie en vertu de la (présente) loi". Cette indépendance ne risque-t-elle pas d'être compromise ou du moins de paraître compromise par la mise sur pied d'une telle procédure consultative? Il sera en tout cas difficile de justifier l'intention d'avoir voulu assurer une pareille surveillance critique à l'égard des activités de la Commission nationale.

Aussi le Conseil d'Etat propose-t-il d'abandonner l'idée d'instituer dans le présent contexte une commission consultative des droits de l'homme. Aux motifs ci-avant déduits s'ajoute que la loi sur la protection des personnes à l'égard du traitement des données à caractère personnel ne saurait être qualifiée de cadre idéal pour servir – en quelque sorte par la tangente – de base légale à la création d'un organe aux missions aussi essentielles.

Article 34

A l'alinéa 2 du paragraphe (2) il est proposé d'intercaler entre les termes „Grand-Duc" et „le serment suivant" les mots „ou de son représentant".

Au paragraphe (6) l'adjectif „assermenté" est à rayer pour être superfétatoire. Il est en effet logique que pour valablement recevoir un serment le président doit lui-même avoir été dûment assermenté. La même remarque est d'ailleurs indiquée à l'endroit de l'article 36, paragraphe (3).

Le Conseil d'Etat se doit enfin de signaler que le vice-président ne figure plus dans le texte de loi à voter. Il n'est plus qu'évoqué au commentaire du paragraphe (2) où il est dit que „le serment du vice-président est réglé de la même manière que celui des autres membres de la Commission nationale".

Article 35

Au paragraphe (7) il se recommande d'écrire „entendue en son avis" au lieu de „demandée en son avis". La révocation d'un membre de la Commission nationale qui dans l'exercice de ses fonctions ne doit recevoir d'instruction de personne (cf. paragraphe (8)) et qui fait partie d'une autorité publique indépendante aussi importante (cf. article 34, paragraphe (1)), doit en effet être entourée d'un maximum de garanties.

Article 36

Au regard du paragraphe (2) le Conseil d'Etat est à se demander si le statut d'employés privés à assimiler à des employés de l'Etat est finalement celui qui convient le mieux aux membres de la Commission nationale, autorité publique censée pouvoir agir en toute indépendance.

Pour le Conseil d'Etat la solution qu'il avait proposée dans son avis du 25 mars 1999 au regard de l'article 9 du projet de loi sur la promotion des droits de l'enfant et la protection sociale de l'enfance lui paraît tout à fait viable *(Doc. parl. 4137[13], sess. ord. 1998-1999).* Dans ce contexte il s'était en effet agi de définir le statut du médiateur auquel il fallait également assurer une indépendance certaine.

A noter que suivant l'article 34, paragraphe (2) les membres de la Commission nationale sont nommés pour un terme de six ans, renouvelable une fois. Le Conseil d'Etat approuve cette limitation de durée de la fonction qui est dans l'intérêt même de la cause. Un renouvellement périodique de la Commission, à des intervalles pas trop éloignés, ne peut que positivement influer sur son fonctionnement et son autorité.

Il ne convient pas de maintenir les membres en fonction au-delà de douze ans. Il n'est partant pas recommandé de leur attribuer le statut de fonctionnaire qui n'est pas spécialement adapté à leur situation. Le Conseil d'Etat se prononce cependant d'ores et déjà contre toute velléité de prolonger la durée de leur mission afin de pouvoir plus facilement justifier une solution consistant à leur reconnaître le statut de fonctionnaire.

Pour les motifs ci-avant déduits sous l'article 34, paragraphe (6) le terme „assermenté" est à biffer au paragraphe (3) de l'article 36.

Article 37

Au regard du paragraphe (1) le Conseil d'Etat renvoie à ses observations à l'endroit de l'article 39 du projet de loi initial et propose le libellé suivant:

> „(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."

L'emploi du terme d'„apport de biens …" paraît en effet trompeur dans le contexte visé alors qu'il rappelle à mauvais escient une notion courante en matière de droit des sociétés.

A l'intérieur du paragraphe (5), il y a lieu d'accorder correctement le participe passé avec son sujet et d'écrire „modifiée" plutôt que „modifié".

Article 39

Le paragraphe (6) dispose en sa deuxième phrase que „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 d'acquittement irrévocable par le juge pénal". La mesure en question, tributaire d'une décision judiciaire d'acquittement définitif risque de perdurer outre mesure. Aussi le Conseil d'Etat propose-t-il d'arrêter les effets de la suspension provisoire ou de la fermeture provisoire *„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"*.

L'hypothèse de non-lieu a été ajoutée dans un souci de protection accrue des droits des justiciables.

Article 41

Le Conseil d'Etat propose de reformuler comme suit le paragraphe (1), alinéa 1er dudit article:

> *„(1) Sans préjudice des dispositions du Code d'Instruction Criminelle, les juges d'instruction, les procureurs d'Etat et leurs substituts accèdent de plein droit, sur requête et par l'intermédiaire de l'Institut luxembourgeois de régulation (ci-après „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."*

L'alinéa 2 reste inchangé alors que d'après le Conseil d'Etat aucun argument ne plaide impérieusement en faveur d'une extension à la centrale des interventions d'urgence 113 des facilités ouvertes à la centrale des secours d'urgence. La police aura toujours le moyen d'accéder aux données en cause en procédant par le biais du ministère public.

Compte tenu de la modification du paragraphe (1) la disposition reprise au paragraphe (3) doit pouvoir être omise, le paragraphe (4) avançant ainsi d'une unité.

Article 44

Cet article dispose dans son paragraphe (2) que „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".

Le texte en question est destiné à répondre à la préoccupation exprimée par le Conseil d'Etat dans son avis du 29 janvier 2002. Dans le but de garantir la validité des règlements grand-ducaux concernant les banques de données pénales et médicales le Conseil d'Etat avait en effet proposé de compléter l'article 42 du projet de loi sous revue par un paragraphe (4) se lisant comme suit:

> „Les articles 12-1 et 28-1 de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques continueront à servir de fondement juridique aux règlements d'application afférents."

Les règlements visés se trouvaient identifiés au commentaire du texte proposé.

Le Conseil d'Etat garde une préférence pour la solution par lui proposée qui peut sans problème être intégrée sous forme de paragraphe (2) à l'article 44, alors que la version proposée par la commission parlementaire lui paraît quelque peu floue. Comment en effet déterminer les règlements „non contraires aux dispositions de la (présente) loi"? Faut-il se référer aux règlements dans leur ensemble? Ou suffit-il au contraire que l'un ou l'autre article de ces actes soit incompatible avec le nouveau texte législatif en voie d'élaboration pour que le règlement en question soit inapplicable en tant que tel et dans sa totalité?

Ainsi délibéré en séance plénière, le 2 juillet 2002.

Le Secrétaire général, — *Le Président,*

Marc BESCH — Marcel SAUBER

Service Central des Imprimés de l'Etat

4735/11

N° 4735[11]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

AMENDEMENTS ADOPTES PAR LA COMMISSION DES MEDIAS ET DES COMMUNICATIONS

DEPECHE DU PRESIDENT DE LA CHAMBRE DES DEPUTES AU PRESIDENT DU CONSEIL D'ETAT

(4.7.2002)

Monsieur le Président,

Me référant à l'article 19 (2) de la loi du 12 juillet 1996 portant réforme du Conseil d'Etat, j'ai l'honneur de vous soumettre ci-après une deuxième série d'amendements au projet de loi sous rubrique, amendements adoptés par la Commission des Médias et des Communications lors de sa réunion du 4 juillet 2002, en présence de M. le Ministre délégué aux Communications qui a apporté l'avis favorable du Gouvernement.

La commission parlementaire a décidé de tenir compte de la plupart des remarques émises par la Haute Corporation dans son avis complémentaire du 2 juillet 2002, à l'exception des remarques concernant les articles 2, 7 (pour ce qui concerne la loi dite ASFT), 10 (1), 14 (1), 28 (2) – et par extension 30 (2) et 32 (11) – 32, 41 et 44.

Afin de permettre à la Haute Corporation de suivre l'agencement du texte complet, la commission souhaite une nouvelle fois joindre, à titre indicatif, le texte coordonné tel qu'il se présente suite à la réunion du 4 juillet 2002. Les commentaires relatifs aux amendements figurent à l'endroit des articles amendés.

*

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

Art. 1er.– ***Objet***

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 et fait respecter les intérêts légalement protégés des personnes morales.

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;

(c) „consentement de la personne concernée“: toute manifestation de volonté expresse, non équivoque, 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;

(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 ou morale est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique;

(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;

(j) „interconnexion“: toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d'autres responsables du traitement;

Commentaire:

Il s'agit d'une part d'assurer la consistance avec l'article 16 (3) qui vise des finalités identiques ou liées. D'autre part, comme la demande d'interconnexion doit émaner conjointement de plusieurs responsables de traitement, la référence à l'article 2 (j) „au même responsable du traitement“ a été supprimée.

En effet, en cas de traitements ayant des finalités liées ou identiques effectués par un seul responsable du traitement, une notification unique ou une autorisation unique sont déjà prévues.

(k) „ministre“: le ministre ayant dans ses attributions la protection des données;

(l) „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, ainsi que des prestations familiales ou d'aides sociales;

(m) „pays tiers“: Etat non membre de l'Union européenne;

(n) „personne concernée“: toute personne physique ou morale, publique ou privée ou groupement de fait qui fait l'objet d'un traitement de données à caractère personnel;

(o) „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;

(p) „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;

(q) „surveillance“: 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;

(r) „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;

(s) „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***

(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.

(2) Sont soumis à la présente loi:

(a) le traitement mis en oeuvre par un responsable du traitement soumis au droit luxembourgeois;

(b) le traitement mis en œuvre par un responsable du traitement, 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 s'applique 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.

(4) La présente loi s'applique à toute forme de captage, de traitement et de diffusion de sons et images qui permettent d'identifier des personnes physiques ou morales.

(5) 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

– au traitement de données concernant une personne morale et dont la publication est prescrite par une loi ou un règlement.

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.

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

(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.

Art. 5.– ***Légitimité du traitement***

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

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

(b) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, ou si

(c) le traitement 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 si

(d) le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, ou si

(e) le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou si

(f) 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.

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:

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

(b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement notamment 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 oeuvre, 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

(f) le traitement mis en oeuvre conformément aux règles de procédures judiciaires en matière civile applicables est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice s'il est mis en oeuvre à cette fin exclusive, 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 et que ce traitement est mis en oeuvre conformément au régime d'autorisation préalable de la Commission nationale tel que prévu à l'article 14, ou lorsque

(h) le traitement est mis en oeuvre par voie de règlement grand-ducal tel que prévu à l'article 17.

(3) L'article 6 paragraphe (1) ne s'applique pas lors d'une procédure judiciaire ou d'une enquête pénale. Toutefois les données génétiques ne peuvent être traitées que 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.

(4) Par dérogation à l'article 6, paragraphe (1), les données génétiques ne peuvent faire l'objet d'un traitement que:

(a) dans les cas visés par les articles 6, paragraphe (2) lettres (c), (f), (g), (h), 6 paragraphe (3) et 7 de la présente loi, ou lorsque

(b) la personne concernée a donné son consentement et si le traitement est effectué dans les seuls domaines de la santé ou de la recherche scientifique sauf indisponibilité du corps humain et 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.

(5) 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 contraire aux dispositions du paragraphe (1) du présent article sous peine d'astreinte.

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

(1) Lorsque le traitement de données tel que défini à l'article 6 paragraphe (1) de la présente loi est 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, de la recherche scientifique dans le domaine de la biologie et de la médecine, le traitement de ces données peut être mis en oeuvre 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 oeuvrant dans les domaines social, familial et thérapeutique, désignées par règlement grand-ducal. Le recours à un sous-traitant est possible dans les conditions prévues à l'article 21.

La commission a certes repris la proposition émise par la Haute Corporation de remplacer les mutuelles par la CMCM. Toutefois, et pour tenir compte des craintes d'abus exprimées dans l'avis complémentaire, les personnes tombant sous l'application de la loi ASFT, devront être désignées par règlement grand-ducal.

(2) Le traitement visé ci-dessus fait l'objet d'une autorisation préalable de la Commission nationale.

(3) Par dérogation au paragraphe (2) qui précède sont soumis à notification:

– le traitement mis en oeuvre conformément à l'article 36 de la loi du 28 août 1998 sur les établissements hospitaliers;

– le traitement mis en oeuvre par un médecin et concernant ses patients.

(4) 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.

(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 contraire aux dispositions du présent article sous peine d'astreinte.

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.

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

(1) Sans préjudice des dispositions prévues dans la législation sur la liberté dans les moyens de communication de masse 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 oeuvre 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;
– lorsque le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou à des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée:

(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;

(e) au droit d'accès de la personne concernée qui peut être différé ou limité conformément à l'article 28, paragraphe (4) et à l'article 29.

(2) Lors de la notification d'un traitement effectué à des fins de journalisme ou d'expression artistique ou littéraire, la notification ne renseigne que sur le(s) nom(s) et adresse(s) du responsable du traitement ou de son représentant.

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 à la sécurité des usagers ainsi qu'à la prévention des accidents, ou

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

(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 oeuvre 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 (3).

(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,

(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.

Art. 11.– ***Traitement à des fins de surveillance sur le lieu du travail***

(1) Le traitement à des fins de surveillance sur le lieu de travail peut être mis en oeuvre, conformément à l'article 14, par l'employeur s'il en est le responsable. Un tel traitement n'est possible que s'il est nécessaire:

(a) pour les besoins de sécurité et de santé des travailleurs, ou

(b) pour les besoins de protection des biens de l'entreprise, ou

(c) pour le contrôle du processus de production portant uniquement sur les machines, ou

(d) pour le contrôle temporaire de production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte, ou

(e) dans le cadre d'une organisation de travail selon l'horaire mobile conformément à la loi.

Dans les cas visés aux lettres (a), (d) et (e), le comité mixte d'entreprise, le cas échéant institué, a un pouvoir de décision tel que défini à l'article 7 paragraphes (1) et (2) de la loi modifiée du 6 mai 1974 instituant des comités mixtes dans les entreprises du secteur privé et organisant la représentation des salariés dans les sociétés anonymes. Le consentement de la personne concernée ne rend pas légitime le traitement mis en oeuvre par l'employeur.

(2) Sans préjudice du droit à l'information de la personne concernée 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.

(3) Quiconque effectue un traitement en violation des dispositions du présent article est puni d'une peine d'emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une des peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte.

Chapitre III.– *Formalités préalables à la mise en oeuvre 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.

(2) Pour les traitements des données dont la mise en œuvre n'est pas susceptible de porter atteinte aux libertés et droits fondamentaux, et notamment à la vie privée, des personnes concernées, la Commission nationale établit et publie des directives en vue d'une notification simplifiée.

Ces directives précisent:

a) la ou les finalités du traitement faisant l'objet d'une notification simplifiée;

b) la ou les catégories de données traitées;

c) la ou les catégories de personnes concernées;

d) les destinataires ou catégories de destinataires auxquels les données sont communiquées;

e) la durée de conservation.

Les traitements qui correspondent à ces directives font l'objet d'une notification simplifiée de conformité envoyée à la Commission nationale le cas échéant par voie électronique.

(3) Est exempté de l'obligation de notification:

(a) le responsable du traitement qui désigne un chargé de la protection des données tenu notamment d'assurer, de manière indépendante, l'application des dispositions légales en la matière et d'établir et de continuer à la Commission nationale un registre des traitements effectués par le responsable du traitement conformément aux dispositions relatives à la publicité des traitements telles que prévues à l'article 15;

(b) le traitement ayant pour seul objet 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) le traitement mis en œuvre conformément aux règles de procédures judiciaires en matière civile et nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice.

(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.

Art. 13.– *Contenu et forme de la notification*

(1) La notification comprend au moins les informations suivantes:

(a) le nom et l'adresse du responsable du traitement, et le cas échéant de son représentant et du sous-traitant;

(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;

(h) la durée de conservation des données.

(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.

(3) La notification se fait auprès de la Commission nationale moyennant support papier ou informatique suivant un schéma à établir par elle. Il est accusé réception de la notification.

(4) Un règlement grand-ducal fixera le montant et les modalités de paiement d'une redevance à percevoir lors de toute notification et de toute modification de notification.

Art. 14.– ***Autorisation préalable de la Commission nationale***

(1) Sont soumis à l'autorisation préalable de la Commission nationale:

(a) les traitements prévus aux articles 6, paragraphe (2), lettres a), b), e), g), 6 paragraphe (4) lettre b), aux articles 7, paragraphe (1), 10 et 11 de la présente loi;

Commentaire:
modifications d'ordre rédactionnel

(b) les traitements de données à des fins historiques, statistiques ou scientifiques visés à l'article 4, paragraphe (2). La Commission nationale vérifie en particulier si ces traitements ne peuvent être réalisés sur base de données rendues anonymes;

(c) l'interconnexion de données à caractère personnel visée à l'article 16;

(d) le traitement concernant le crédit et la solvabilité des personnes concernées;

(e) 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.

(2) La demande d'autorisation comprend les informations suivantes:

(a) le nom et l'adresse du responsable du traitement ou de son représentant et le cas échéant du sous-traitant;

(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 aux articles 22 et 23;

(j) la durée de conservation des données.

(3) 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.

(4) 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.

Commentaire:
la commission se rallie à l'avis du Conseil d'Etat et redresse la faute de frappe.

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

(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 (3) lettre (a).

(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,

(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 de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi,

(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***

(1) L'interconnexion de données qui n'est pas expressément prévue par un texte légal doit faire l'objet d'une autorisation préalable de la Commission nationale sur demande conjointe présentée par les responsables des traitements en cause.

(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.

(3) L'interconnexion n'est autorisée que dans le respect des finalités identiques ou liées de fichiers et 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 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 (OIP-Interpol).

(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 ci-dessus.

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.

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 traitement contraire aux dispositions des paragraphes (1), (2) et (4) du présent article sous peine d'astreinte.

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

(f) le transfert intervienne depuis un registre public tel que prévu à l'article 12, paragraphe (3) lettre (b).

(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 notifier à la Commission nationale un rapport établissant les conditions dans 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 traitement contraire aux dispositions du présent article sous peine d'astreinte.

Art. 20.– ***Information réciproque***

(1) La Commission nationale informe le ministre de toute décision prise en application de l'article 18, paragraphes (3) et (4) et de l'article 19 paragraphes (1) et (2). Le ministre en informe la Commission européenne.

(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*

(1) Le responsable du traitement doit mettre en œuvre toutes les mesures techniques et d'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. Ces mesures font l'objet d'un rapport annuel à soumettre par le responsable du traitement 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 oeuvre, 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 services 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.

(4) Le responsable du traitement agissant dans le cadre de l'accomplissement de ses missions visées à l'article 7, paragraphe (1), 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.

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;
- la durée de conservation 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;
- la durée de conservation 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.

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;

(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 de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi;

(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,

(2) Les dispositions de l'article 26 sont susceptibles de dérogations lors de la collecte de données dans les conditions prévues à l'article 9, paragraphe (1) lettre (c).

(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.

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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte.

(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 de son tuteur.

(4) Toute personne a un droit d'accès aux données la concernant et utilisées aux fins d'un traitement mis en oeuvre dans le cadre de la liberté d'expression tel que prévu à l'article 9. Aussi longtemps que les

données auxquelles l'accès est demandé n'ont pas été publiées, la communication de ces données, ainsi que toute information disponible sur leur origine ne peut se faire que par l'intermédiaire de la Commission nationale qui opère conformément à l'article 9, paragraphe (3) de la présente loi.

(5) 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.

(6) 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.

(7) Toute rectification, tout effacement ou verrouillage effectué conformément au paragraphe (5) 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.

(8) Sans préjudice de la sanction prévue au paragraphe (5), 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte.

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;

(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 de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi;

(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 et que la mesure d'exception est prise conformément à l'article 28, paragraphe (4);

(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).

(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.

(3) 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.

(4) 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.

(5) Quiconque contrevient à la disposition du paragraphe (3) 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 (3) du présent article sous peine d'astreinte.

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 oeuvre par le responsable du traitement ne peut pas porter sur ces données;

(b) de s'opposer, sur demande et gratuitement, au traitement la concernant envisagé par le responsable du traitement 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte.

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.

(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 oeuvre 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 oeuvre des traitements soumis au régime de l'article 14 de la présente loi;

(e) être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi. Ces avis sont publiés au rapport annuel visé à l'article 15, paragraphe (6);

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

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

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

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

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

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

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

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

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

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

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

(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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte.

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.

Commentaire:

consistance avec la définition de l'article 2 (k).

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.

En cas de cessation du mandat, il est réintégré sur sa demande dans son administration d'origine à un emploi correspondant au traitement qu'il a touché précédemment, augmenté des échelons et majorations de l'indice se rapportant aux années de service passées comme Président ou membre effectif jusqu'à concurrence du dernier échelon du grade.

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 sont des experts indépendants dont l'indemnité est fixée par règlement grand-ducal.

Commentaire:

texte proposé par le Gouvernement afin de tenir compte de la suggestion du Conseil d'Etat de s'inspirer du projet de loi 4137.

Les paragraphes (3) et (6) ont été intégrés au paragraphe (2) et sont devenus les alinéas 2 et 4, alinéa 2 étant celui du paragraphe 2, alinéa 2 du texte soumis à l'avis complémentaire du Conseil d'Etat.

(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***

(1) Le cadre du personnel de la Commission nationale comprend les fonctions et emplois suivants:

Dans la carrière moyenne de l'administration, grade de computation de la bonification d'ancienneté: grade 7, carrière du rédacteur:

- 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 de la carrière moyenne des rédacteurs sont des fonctionnaires de l'Etat en ce qui concerne notamment leur statut, leur traitement et leur régime de pension qui est régi par les dispositions légales régissant les 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.

Commentaire:

texte proposé par la commission, sur avis favorable du Gouvernement, dans la lignée de l'amendement prévu à l'article 34. Les paragraphes (4) et (6) deviennent les paragraphes (3) et (4). Le paragraphe (5) du texte coordonné soumis à l'avis complémentaire du Conseil d'Etat a été suprimé.

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.

(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 à l'article 13 de la présente loi. Pour le solde des frais restant à couvrir dans le cadre de ses missions conférées par la présente loi, la Commission nationale bénéficiera d'une dotation d'un montant à déterminer sur une base annuelle et à inscrire au budget de l'Etat.

(5) La loi du 27 novembre 2001 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2002 est modifiée comme suit: il est ajouté au budget des dépenses au Chapitre III - Dépenses courantes sous „00 - Ministère d'Etat" une section „00.9 Commission nationale pour la protection des données" émargeant les articles suivants:

„12.300: Prise en charge par l'Etat des frais encourus par la Commission nationale pour la protection des données. (crédit non limitatif et sans distinction d'exercice) 200.870

33.000: Dotation initiale en faveur de la Commission nationale pour la protection des données..... 200.000"

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***

(1) Tout responsable de traitement peut, dans le cadre de l'article 12, paragraphe (3) sous (a), et aux fins y visées, 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.

(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:

(a) il ne connaît aucun lien de subordination vis-à-vis du responsable du traitement et ne peut être lié au responsable du traitement par un contrat de travail:

(b) il ne peut être révoqué pour des raisons liées à l'exercice de ses missions, hormis le cas de la violation de ses obligations légales ou conventionnelles.

(4) Le chargé de la protection 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.

(5) 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.

(6) 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 ainsi que d'assises financières d'une valeur de 20.000 euros.

(7) 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.

(8) La Commission nationale vérifie les qualités de tout chargé de la protection des données.

Elle peut s'opposer à tout moment à la désignation ou au maintien du chargé de la protection des données lorsqu'il:

(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 ~~à caractère personnel~~ 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.

(9) La Commission nationale définit les modalités du contrôle continu des qualités requises à la fonction de chargé de la protection des données.

(10) 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 (ci-après „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.

La centrale des secours d'urgence 112 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.

(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 et de la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg.

Commentaire:

il s'agit de tenir compte du fait que la centrale téléphonique du service d'incendie et de sauvetage précité effectue les mêmes interventions que la centrale des secours d'urgence 112.

(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.

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).

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 ne 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.

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.

*

Au nom de la Commission précitée je vous saurais gré de bien vouloir m'envoyer dans les meilleurs délais l'avis du Conseil d'Etat sur les amendements exposés ci-dessus, afin de permettre à la Chambre des Députés de voter le projet de loi avant les vacances parlementaires.

Copie de la présente est envoyée pour information au Premier Ministre, Ministre d'Etat, au Ministre délégué aux Communications et au Ministre aux Relations avec le Parlement.

Veuillez agréer, Monsieur le Président, l'expression de ma considération très distinguée.

Jean SPAUTZ
Président de la Chambre des Députés

Service Central des Imprimés de l'Etat

4735/12

N° 4735[12]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

DEUXIEME AVIS COMPLEMENTAIRE DU CONSEIL D'ETAT

(9.7.2002)

Sur la base de l'article 19(2) de sa loi organique du 12 juillet 1996, le Conseil d'Etat fut saisi en date du 4 juillet 2002 par le Président de la Chambre des députés d'amendements au projet de loi sous rubrique, adoptés le même jour par la Commission des médias et des communications de la Chambre des députés.

Les amendements intégrés dans une nouvelle version coordonnée étaient accompagnés d'un commentaire.

Le Conseil d'Etat constate que les amendements en question s'inspirent pour la plupart de son avis complémentaire du 2 juillet 2002.

Il se contente par conséquent de consacrer quelques développements aux sanctions pénales et de faire une remarque par rapport aux membres suppléants de la Commission nationale, tout en regrettant sérieusement de ne pas avoir été suivi dans sa proposition de texte concernant l'article 44, paragraphe (2) qui était de nature à éviter l'insécurité juridique dont restera affectée la version retenue par la commission parlementaire.

Quant aux sanctions pénales, il y a lieu de souligner que la peine accessoire de la fermeture d'un établissement fautif a été abandonnée pour être remplacée par la possibilité, pour la juridiction saisie, de prononcer la cessation du traitement illégal sous peine d'astreinte.

Si ce changement d'optique va dans la bonne direction, il n'en demeure pas moins qu'il n'est pas susceptible d'avoir un effet utile dans toutes les circonstances visées. Il convient partant de nuancer et de sélectionner soigneusement les hypothèses dans lesquelles cette mesure peut effectivement s'appliquer.

Ne posent pas problème à cet égard les dispositions des articles 4, paragraphe (3), 5, paragraphe (2), 8, paragraphe (4), 10, paragraphe (4), 11, paragraphe (3), 12, paragraphe (4), l4, paragraphe (4), 17, paragraphe (3), 25, 26, paragraphe (3) et 27, paragraphe (4), sauf qu'il y a lieu d'y préciser systématiquement „sous peine d'astreinte *dont le maximum est fixé par ladite juridiction*". A l'article 6, paragraphe (5) il se recommande de libeller comme suit la phrase finale:

> „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.*"

Par analogie, l'article 7, paragraphe (5) *in fine* est à rédiger en ces termes:

> „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.*"

La phrase finale de l'article 18, paragraphe (5), est à libeller comme suit:

> „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.*"

Dans la même optique, l'article 19, paragraphe (4), prendra la teneur suivante:

„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.*"

Par contre, le contexte des articles 28, paragraphes (2) et (8), 29, paragraphe (5), 30, paragraphe (2) et 32, paragraphe (11) ne se prête guère au maintien de la peine d'astreinte. Les dispositions en cause traitent en effet respectivement du droit d'accès et du droit d'opposition de la personne concernée ou encore des missions et pouvoirs de la Commission nationale, matières où il paraît difficile de concevoir le traitement illégal à faire cesser et sanctionner moyennant peine d'astreinte. Aussi le Conseil d'Etat en préconise-t-il l'abandon dans le cadre des dispositions susvisées.

Quant à l'article 34, le Conseil d'Etat estime qu'il y a lieu de remplacer le dernier alinéa du paragraphe (2) par la disposition suivante:

„Les membres suppléants touchent une indemnité dont le montant est fixé par règlement grand-ducal."

Le Conseil d'Etat termine par quelques remarques d'ordre formel.

Il se doit de signaler d'abord quelques fautes de frappe en rapport avec les dispositions suivantes:

A l'article 3, paragraphe (2), lettre (b), il convient d'intercaler le pronom „qui" devant la virgule introduisant l'incidente débutant par les mots „sans être établi sur le territoire luxembourgeois …".

A l'article 8, paragraphe (2), il s'agit de redresser une faute d'inadvertance et d'écrire „d'une disposition légale".

A l'article 9, paragraphe (1) lettre (d), il y a lieu de mettre „(d) à l'obligation …".

A l'article 17, paragraphe (1), lettre (a), il y a lieu d'écrire „…, de l'Inspection générale de la police …".

Il se recommande encore dans le contexte de l'article 34, paragraphe (2) – par remplacement du signe des deux points par un point-virgule – de réagencer comme suit l'alinéa 7:

„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."

Il s'entend que d'autres corrections d'orthographe ou de ponctuation pourraient être effectuées sans façon et sans faire l'objet d'amendements formels.

Reste à rectifier deux erreurs de renvoi. A l'article 10, paragraphe (2) *in fine*, il faut mentionner l'article 26, paragraphe *(2)* au lieu du paragraphe (3). Dans le cadre de l'article 28, paragraphe (4), il convient de biffer le passage „qui opère conformément à l'article 9, paragraphe (3) de la présente loi", alors que dans le contexte des amendements du 6 juin 2002 ledit paragraphe (3) a précisément été éliminé du projet de loi sous examen.

Le Conseil d'Etat suggère enfin d'adopter à travers l'ensemble du projet une structure uniforme de présentation des chapitres et articles avec les intitulés correspondants.

Ainsi délibéré en séance plénière, le 9 juillet 2002.

Le Secrétaire général, *Le Président,*
Marc BESCH Marcel SAUBER

4735/13

N° 4735[13]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

RAPPORT DE LA COMMISSION DES MEDIA ET DES COMMUNICATIONS

(10.7.2002)

La Commission se compose de: M. Laurent MOSAR, Président; M. Patrick SANTER, Rapporteur; Mme Simone BEISSEL, M. Alex BODRY, Mme Mady DELVAUX-STEHRES, MM. Robert GARCIA, Marcel GLESENER, Fernand GREISEN, Jean-Marie HALSDORF, Paul HELMINGER et Jean-Paul RIPPINGER, Membres.

*

TABLE DES MATIERES

Prolégomènes

A. Antécédents procéduraux

B. Un équilibre entre société de l'information et protection de la vie privée

C. Les concepts clés

I. Le champ d'application

A. Le champ d'application matériel et personnel

B. Le champ d'application territorial

II. Les conditions du traitement

A. Le principe de la finalité du traitement

B. Conditions spécifiques à certains traitements

III. Les droits de la personne concernée

A. Le droit à l'information

B. Le droit d'accès

C. Le droit d'opposition

D. Les décisions individuelles automatisées

IV. Les formalités de mise en œuvre du traitement

A. Le principe: la notification préalable du traitement

B. L'exception: l'autorisation préalable du traitement

C. Le registre public

V. Le contrôle du traitement

A. Le contrôle externe: la Commission nationale pour la protection des données

B. Le contrôle interne

VI. Les recours juridictionnels

A. Les recours de droit commun

B. L'action en cessation

VII. Le transfert de données vers un pays tiers
A. Principes
B. Exceptions
VIII. Les dispositions pénales
IX. Une disposition spécifique et exceptionnelle: l'article 41
X. Dispositions transitoires et finales; entrée en vigueur
Conclusion

*

PROLEGOMENES

A. Antécédents procéduraux

Le projet de loi 4735 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel transpose en droit luxembourgeois la directive 95/46/CE du Parlement Européen et du Conseil du 24 octobre 1995[1] (ci-après la „directive").

Il ne s'agissait pas de la première tentative de transposition de la directive dans notre droit. Dans un premier temps, le gouvernement entendait procéder à une transposition, certes partielle, de la directive afin de remplacer le plus rapidement possible la loi modifiée du 31 mars 1979 déjà obsolète à l'époque[2].

Le gouvernement ayant décidé de déposer un projet de loi portant transposition intégrale de la directive, le présent projet 4735, le projet de transposition partielle 4357 a été retiré du rôle en mai 1998.

Le projet de loi sous rubrique a été déposé par Monsieur le Ministre délégué aux Communications le 7 décembre 2000. Les chambres professionnelles et autorités suivantes ont émis leurs avis:

– la Chambre des fonctionnaires et employés publics le 22 mai 2001,
– Monsieur le Procureur général d'Etat le 5 juillet 2001,
– la Chambre des employés privés le 30 octobre 2001,
– la Chambre de travail le 14 novembre 2001,
– la Chambre des métiers le 22 novembre 2001, et
– la Chambre de commerce le 13 février 2002.

L'avis du Conseil d'Etat est intervenu le 29 janvier 2002 et a été, ensemble avec le projet de loi et les avis précités, minutieusement examiné par la Commission des média et des communications (ci-après la „commission") dans ses réunions du 9 mars 2002 lors de laquelle Monsieur Patrick Santer a été désigné rapporteur, et des 20 mars, 21 mars, 11 avril, 2 mai, 10 mai, 13 mai, 16 mai et 30 mai 2002.

Le 28 mai 2002, la commission a eu une entrevue avec Monsieur le Procureur d'Etat Robert Biever et avec Monsieur le Premier Avocat Général Georges Wivenes. Le 5 juin 2002, elle a adopté des amendements qui ont été avisés par le Conseil d'Etat dans son avis complémentaire du 2 juillet 2002. Cet avis complémentaire a été discuté par la commission lors de sa réunion du 4 juillet 2002. Le 4 juillet 2002, la commission a présenté des amendements au Conseil d'Etat qui furent avisés par celui-ci dans son deuxième avis complémentaire du 9 juillet 2002. Le 10 juillet 2002, la commission a adopté à l'unanimité le présent rapport.

L'article 11 du projet de loi régissant la surveillance sur le lieu de travail a été avisé par la commission du Travail et de l'Emploi. Son avis du 15 mai 2002 est reproduit au document parlementaire 4735[7].

Les Etats membres auraient dû transposer jusqu'au 24 octobre 1998 la directive en droit luxembourgeois[3].

N'ayant pas transposé la directive dans ce délai, le Luxembourg a été condamné par la Cour de Justice des Communautés Européennes par arrêt du 4 octobre 2001[4].

---

1 Pour le texte de la directive: doc. parl. 4735, p. 53

2 Projet de loi 4357

3 Directive, article 32

4 Aff C-450/00

Pour être complet, il convient de signaler que la directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications doit encore être transposée en droit luxembourgeois[1].

Un recours vient d'être introduit contre le Luxembourg pour non-transposition en date du 4 juin 2002[2].

B. Un équilibre entre société de l'information et protection de la vie privée

Quiconque lit aujourd'hui la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques[3], ne peut que constater son obsolescence au regard de l'évolution technologique qui se poursuit depuis quelques années déjà. Cette loi soumet à autorisation ministérielle préalable, après avis préalable d'une commission consultative, la création et l'exploitation de toute banque de données nominatives ne relevant pas de l'Etat. Le caractère illusoire de l'application quotidienne de cette loi ne fait pas de doute.

Adaptée à son époque, elle a été dépassée en raison de l'omniprésence de l'informatique dans notre vie tant professionnelle que privée. Alors qu'à la fin des années 1970, les systèmes informatiques étaient encombrants, peu flexibles et chers, l'apparition des ordinateurs personnels de plus en plus performants[4], leur démocratisation et l'explosion des services multimédia ont fait de l'ordinateur un outil indispensable à la vie quotidienne. A tel point d'ailleurs que d'aucuns ont relevé l'existence d'une „fracture informatique" entre ceux qui savent manier un ordinateur et ceux qui ne le savent pas. „Ainsi on est passé d'une société dans laquelle l'informatique était un outil au service des activités humaines à une société de l'information entraînant des modifications structurelles de nos modes de vie."[5]

L'omniprésence de l'informatique pour bénéfique qu'elle soit recèle des dangers souvent ignorés pour ce qui est de la protection des données à caractère personnel. La personne sujet de l'information – la personne concernée – peut-elle garder la maîtrise sur ce qu'adviendra de son „double informationnel"? Celui-ci ne risque-t-il pas d'être faussé ou utilisé à des fins non voulues? „L'individu est, en effet, traqué de nos jours dans ses secrets les plus intimes par l'indiscrétion totale croissante tenant à des raisons diverses: contrôles administratifs, intérêts commerciaux, motifs de recherche."[6] Ces dangers vont croître avec le développement du commerce électronique. „De fait, le commerce électronique favorise la collecte de données personnelles, notamment sur les visiteurs de sites constitués par les entreprises, ou sur les clients. Les visiteurs et les clients sont d'ailleurs, souvent, sollicités lorsqu'ils reviennent sur un site, au moyen des „cookies" qui ont été implantés sur le disque dur de leur ordinateur lors de leur précédent passage. Les préoccupations pour la protection des personnes que suscitent ces pratiques, et d'autres encore, ont été débattues lors du sommet organisé par l'OCDE à Ottawa en 1998, et l'une des résolutions adoptées à cette occasion est „relative à la protection de la vie privée sur les réseaux mondiaux" (V. Rev. dr. informatiq. et télécoms, 1998-3, pp. 1001 s.)."[7] La directive et la directive 97/66/CE, dont la transposition ne saurait tarder, trouveront une solution à cette préoccupation.

Dans la mesure où „le partage et la communication internationale de données sont devenus la règle et non l'exception"[8], deux tendances s'opposent. La première est de dire qu'il s'agit là du prix à payer, d'un sacrifice à supporter si l'on veut profiter des avantages procurés par l'informatique. La seconde est de trouver un équilibre entre la libre circulation des données à caractère personnel et la protection des libertés et droit fondamentaux de la personne concernée.

---

1 JOCE L24 du 30 janvier 1998

2 affaire C-211/02

3 Modifiée par les lois des 19 novembre 1987, 30 septembre 1992, 1er octobre 1992 et 9 août 1993

4 Plus d'un milliard d'ordinateurs personnels ont été vendus depuis 1971. Le deuxième milliard sera atteint d'ici 2007/2008 (source agence de presse dpa du 2 juillet 2002)

5 Doc. parl. 4735, p. 80

6 Commission nationale Informatique et Libertés (CNIL) (France), Dix ans d'informatique et libertés, Economica, 1988, p. 15

7 Huet, Etude relative aux contrats encadrant les transferts de données personnelles entre les parties à la Convention 108 et les pays tiers n'offrant pas un niveau de protection adéquat, 7-9 février 2001, www.legal.coe.int.

8 Havelange, Lacoste, Les flux transfrontaliers de données à caractère personnel en droit européen, JTDE 2001, p. 241

En effet, le respect de ces droits et libertés, parmi lesquels le droit à la vie privée, constitue un fondement de notre Etat de droit. L'article 8 de la Charte des droits fondamentaux de l'Union Européenne annexée au traité de Nice[1] reconnaît expressément le droit à la protection des données à caractère personnel. Celui-ci doit également être rangé parmi les „droits naturels et la personne humaine et de la famille" dont l'Etat doit garantir le respect en vertu de l'article 11 (3) de la Constitution ou – pour reprendre la formulation proposée par la Chambre des Députés dans le cadre de la révision de l'article 11 – parmi les „droits fondamentaux de la personne humaine"[2].

C'est cette seconde voie, à savoir celle de la conciliation entre les deux objectifs, qui a été, à juste titre, choisie par la directive, comme le démontre son intitulé, puisqu'elle est „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".

La directive reprend l'option choisie en son temps par la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, entrée en vigueur le 1er octobre 1985[3].

La directive part du constat que les flux transfrontaliers de données à caractère personnel vont augmenter avec la continuation de l'intégration économique et le fonctionnement du marché intérieur ainsi qu'avec le renforcement de la coopération scientifique et technique et la mise en place de nouveaux réseaux de télécommunications dans la Communauté Européenne. Cependant, elle relève que les disparités dans les dispositions nationales quant au niveau de protection des droits et libertés des personnes à l'égard de traitement de données à caractère personnel „peuvent empêcher la transmission de ces données du territoire d'un Etat membre à celui d'un autre Etat membre; que ces différences peuvent dès lors constituer un obstacle à l'exercice d'une série d'activités à l'échelle communautaire, fausser la concurrence et empêcher les administrations de s'acquitter des responsabilités qui leur incombent en vertu du droit communautaire"[4].

Une coordination au niveau communautaire des législations nationales s'imposait. La directive vise à concilier la libre circulation des données au sein de l'Union Européenne et la protection des droits et libertés des personnes concernées. La directive tend à l'établissement d'un „niveau élevé de protection dans la Communauté"[5]. Cet équilibre, certes délicat, se retrouve dans le projet de loi 4735.

Loin de les rendre superflus, „les principes de la protection des droits et libertés des personnes, notamment du droit à la vie privée, contenus dans la (…) directive précisent et amplifient ceux qui sont contenus" dans la Convention 108 du Conseil de l'Europe[6].

C. Les concepts clés

La compréhension de la portée du projet de loi 4735 suppose la connaissance d'un certain nombre de concepts clés qui reviendront tout au long du texte du projet de loi.

1) Le consentement de la personne concernée (article 2, lettre (c))

Il s'agit d'une notion essentielle de la loi à venir. Ainsi, par exemple, un tel consentement permet de légitimer un traitement[7] ou de transférer des données n'assurant pas un niveau de protection adéquat[8]. Ce principe n'est cependant pas général[9].

Le consentement de la personne au traitement de ses données doit être exprès et non équivoque. Aucune forme écrite et aucune formule sacramentelle ne sont requises.

---

1 JOCE du 18 décembre 2000 C-364/10

2 Doc. parl. 3923 B-2

3 Cette convention a été ratifiée par 28 Etats membres du Conseil de l'Europe (situation au 12 juin 2002, source: www.coe.int). Le Luxembourg a ratifié la Convention 108 le 10 février 1988. A noter qu'un protocole additionnel à la Convention 108 a été ouvert à la signature le 8 novembre 2001. Au 12 juin 2002, le Luxembourg n'a pas encore signé ce protocole additionnel.

4 Directive, considérant 7

5 Directive, considérant 10

6 Directive, considérant 11

7 Art. 5 (1) lettre (f)

8 Art. 19 (1) lettre (a)

9 Voir art. 6, paragraphe (1) lettre (a), 6, paragraphe (4) lettre (b), 11 paragraphe (1)

Le consentement doit être libre. Les auteurs du projet de loi ont cru pertinent de procéder à une appréciation critique de la liberté du consentement. Ils soulignent qu'en présence d'une situation dans laquelle le responsable du traitement se trouve en position de force face à la personne concernée, comme par exemple lorsque la personne concernée souhaite obtenir un prêt bancaire ou souscrire une assurance-vie, il peut „s'avérer fort probable que le consentement de la personne concernée n'est pas forcément libre"[1].

La liberté du consentement doit s'apprécier au cas par cas au regard des circonstances de l'espèce. Pour ce faire, les articles 1112 et suivants du Code civil tels qu'appliqués par la jurisprudence[2] serviront de lignes directrices en la matière.

Le consentement doit être spécifique, en ce qu'il ne peut porter que sur des traitements déterminés. C'est dans cette optique que le responsable du traitement doit informer la personne concernée sur la ou les finalités déterminées du traitement auquel les données sont destinées[3]. Si plusieurs finalités sont poursuivies par un même traitement, le responsable du traitement doit en informer la personne concernée[4].

Finalement le consentement doit être informé. La personne concernée doit donner son consentement en connaissance de cause, ce qui explique une nouvelle fois le lien entre le consentement de la personne concernée avec le principe de la qualité des données prévu à l'article 4, paragraphe (1) lettre (a), et avec le droit à l'information prévu à l'article 26. Ce droit à l'information doit s'exercer soit lors de la collecte des données auprès de la personne concernée, soit lors de l'enregistrement ou la première communication à un tiers pour les données qui n'ont pas été collectées auprès de la personne concernée.

2) La donnée à caractère personnel – la donnée (article 2, lettre (e))

Il y a donnée lorsqu'une information quels que soient sa nature ou son support concerne une personne identifiée ou identifiable. „Une personne 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"[5], comme par exemple le numéro de passeport, un numéro de téléphone ou celui d'une plaque minéralogique.

Une donnée codée tombe dans la définition précitée, dès lors que la personne concernée peut être identifiée ou identifiable[6]. L'identification peut se faire par „toute forme de captage, de traitement et de diffusion de sons ou d'images"[7].

Une donnée anonyme en est au contraire exclue. Une donnée rendue anonyme également, mais uniquement à partir du moment où elle a été rendue anonyme, à condition qu'on ne puisse plus procéder à l'identification de la personne concernée.

Pour être réputée anonyme ou rendue anonyme, il faut qu'il s'agisse d'une donnée pour laquelle il n'existe aucun moyen technique, soit dans le chef du responsable du traitement, soit même dans le chef d'un tiers, permettant de rattacher cette donnée à un individu[8]. Il appartient au responsable du traitement d'apporter la preuve que les données qu'il traite sont à qualifier de données anonymes[9].

3) Le fichier (article 2, lettre (h))

Un tel fichier doit être structuré pour que le projet de loi trouve à s'appliquer. Le projet de loi ne s'applique donc pas à n'importe quel fichier. Peu importe la structure appliquée à un tel fichier. Il s'agit de la définition utilisée à l'article 2 c) de la directive[10].

---

1 Doc. parl. 4735, p. 27

2 Voir p.ex. Cour 6 octobre 1993, Pas. 29, 279

3 Voir article 26

4 Sur les finalités induites: voir II. A. 1) a

5 Article 2 lettre (e)

6 Leonard, Poullet, La protection des données à caractère personnel en pleine (r)évolution, JT 1999, p. 377, part. p. 378, note (16)

7 Article 3, paragraphe (4)

8 Directive, considérant 26

9 Doc. parl. 4735, p. 25

10 Voir aussi article 3, paragraphe (1)

4) L'instance médicale (article 2, lettre (i))

Dans son avis complémentaire du 2 juillet 2002, le Conseil d'Etat a émis des doutes sur les conséquences de l'inclusion de la loi du 28 août 1998 sur les établissements hospitaliers à l'endroit de l'article 2, lettre (i). La commission maintient la définition de l'instance médicale, alors que celle-ci a précisément été confortée par les instances gouvernementales compétentes.

5) Le responsable du traitement (article 2, lettre (o))

Le responsable du traitement dispose du pouvoir décisionnel pour déterminer les finalités poursuivies par un traitement et les moyens à mettre en œuvre en vue de ce traitement. Il se distingue ainsi du sous-traitant[1] chargé de l'exécution matérielle de tout ou partie du traitement.

Un même traitement peut être soumis conjointement à plusieurs responsables d'un traitement. Si, par exemple, plusieurs sociétés d'assurance ou de réassurance décident de s'associer pour couvrir une catégorie particulière de risques sans créer pour ce faire une entité juridique distincte, elles seront chacune considérées comme responsable du traitement pour les données traitées dans le cadre de cette association.

6) Le traitement (article 2, lettre (s))

Le traitement remplace la notion de „banque de données" utilisée par la loi du 31 mars 1979. C'est en effet non la création d'une „banque de données", comprise comme lieu où les données sont conservées, mais le traitement de ces données qui peut donner lieu à des abus. La focalisation s'est déplacée du lieu de stockage des données au traitement de celles-ci.

*

Deux remarques pour terminer cette introduction:

D'une part, le langage courant désigne cette matière sous le terme générique de „protection des données". Or le présent projet de loi n'a pas pour objet de protéger les données. Il faut au contraire protéger les personnes dont les données qui font l'objet d'un traitement contre tout abus en la matière pour assurer le respect de leurs droits et libertés fondamentales.

D'autre part, il a été reproché au projet de loi sous rubrique d'être un „fourre-tout" de dispositions et qu'il aurait été plus approprié de suivre une approche „sectorielle" au lieu d'édicter un texte à vocation horizontale. La commission approuve l'option du gouvernement, dans la mesure où tout un chacun retrouve dans un seul et même texte l'ensemble des dispositions concernant le traitement des données[2].

*

I. LE CHAMP D'APPLICATION

A. Le champ d'application matériel et personnel

Tout en transposant la directive en droit luxembourgeois, le projet de loi va parfois au-delà de ce qui est exigé dans le texte communautaire.

Ainsi le champ d'application de la directive a-t-elle été élargi par le projet de loi aux intérêts légalement protégés des personnes morales[3]. Les intérêts légalement protégés des personnes morales constituent le pendant des libertés et droits fondamentaux de la personne physique.

Il serait faux de croire que le bénéfice de la protection assurée par le biais du présent projet de loi soit dépendant de l'existence de la personnalité juridique. Ainsi les groupements de fait, dépourvus d'une telle personnalité juridique, doivent être comptés parmi les personnes concernées[4].

Le champ d'application personnel est donc suffisamment vaste.

---

1 Défini à l'article 2, lettre (p)

2 Par la suite, nous utiliserons les termes tels que définis à l'article 2 de la directive

3 Article 1er. La législation belge continue d'exclure les personnes morales de son champ d'application: Léonard et Poullet, op. cit., JT 1999, p. 380

4 Article 2, lettre (n)

En ce qui concerne le champ d'application matériel, la défense, la sécurité publique, la sûreté de l'Etat et les activités de l'Etat dans le domaine pénal, qui ne sont abordées par la directive qu'à titre facultatif, sont intégrées dans le champ d'application du projet de loi, comme cela avait d'ailleurs déjà été le cas pour la loi du 31 mars 1979[1]. La loi de 1979 se trouve cependant précisée sur ce point, comme nous le verrons par après.

Toujours en ce qui concerne le champ d'application *ratione materiae*, l'article 3, paragraphe (1), ainsi que l'article 2, lettre (s), précisent que le traitement n'a pas besoin d'être entièrement automatisé. „Si au moins une des opérations, dont l'ensemble constitue le traitement tel que défini à l'article 2 du présent projet, est effectuée de façon automatisée, les autres l'étant de façon „manuelle", le traitement doit être opéré en conformité avec les dispositions de la présente loi[2]." Ainsi, par exemple, si les données sont collectées par un sondeur lors d'un entretien avec la personne concernée sur base d'un formulaire avec des cases à cocher, mais que leur enregistrement est effectué de manière automatisée, les dispositions du projet de loi s'appliquent.

A cela s'ajoute que même en présence d'un traitement non automatisé le projet de loi retrouve application, dès lors que les données ainsi traitées figurent ou sont appelées à figurer dans un fichier. Un tel fichier doit être structuré „selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause"[3]. Ainsi, un fichier manuel peut être considéré comme structuré au sens du projet de loi et de la directive, si, par exemple, il range les noms des personnes concernées par ordre alphabétique. Comme indiqué précédemment ce n'est que le fichier absolument dénué de toute structuration qui échappe au projet de loi.

L'article 3, paragraphe (5), exclut deux catégories de traitement de son champ d'application.

Il s'agit, d'une part, d'écarter, au nom du respect dû à la vie privée, du champ d'application du projet de loi les traitements mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, par exemple, la correspondance ou la tenue d'un répertoire d'adresses[4]. Dès que le traitement ne vise plus exclusivement les activités personnelles ou domestiques d'une personne physique et est utilisé, ne serait-ce que partiellement pour une activité professionnelle ou sort, ne serait-ce que provisoirement, de la sphère privée de cette personne, les dispositions du projet s'appliquent.

D'autre part, ne sont également pas couverts par le projet de loi les traitements concernant une personne morale dont la publication est requise par la loi ou un règlement. Sont plus particulièrement visées les données des personnes morales qui doivent être publiées au Mémorial en application de la loi modifiée du 10 août 1915 sur les sociétés commerciales.

B. Le champ d'application territorial[5]

Le champ d'application *ratione loci* est déterminé par l'article 3, paragraphe (2) du projet de loi. Cette disposition est particulièrement importante au regard de la libre circulation des données au sein de l'Union européenne. Elle vise à éviter à la fois les situations où aucune législation sur la protection des données ne s'applique et les situations dans lesquelles deux ou plusieurs législations nationales viendraient à s'appliquer cumulativement.

1. Le responsable du traitement soumis au droit luxembourgeois (article 3, paragraphe (1) lettre (a))

Le projet de loi s'applique au traitement effectué par un responsable du traitement soumis au droit luxembourgeois. Est soumis au droit luxembourgeois le responsable du traitement qui est établi au Luxembourg. L'article 3, paragraphe (1) lettre (a), reprend les dispositions de l'article 3, paragraphe (1),

---

1 Voir article 12 de la loi de 1979

2 Doc. parl. 4735, p.28

3 Directive, considérants 15 et 27

4 Directive, considérant 12

5 Pour la détermination du champ d'application de la directive à des sites Internet localisés en dehors de l'Union Européenne: voir rapport du groupe institué à l'article 29 de la directive adopté le 30 mai 2002 („Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU web sites 5035/01/EN/Final WP56, www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm)

lettre (a) et lettre (b), premier tiret, du texte soumis par la commission au Conseil d'Etat le 5 juin 2002. Le second tiret du paragraphe (3) lettre (b) devient le paragraphe (3) lettre (b) à lui tout seul.

La version initiale du projet de loi, plus proche de l'article 4 de la directive, exigeait que le responsable du traitement soit „établi sur le territoire luxembourgeois ou en un lieu où, selon le droit international public, est applicable le droit luxembourgeois". Le texte adopté par la commission qui, plus concis, se contente de prévoir que le responsable du traitement doit être soumis au droit luxembourgeois, c'est-à-dire établi sur le territoire luxembourgeois sans référence au droit international public. Cette différence avec le texte initial ne prête à aucune conséquence.

Partant, sont concernés les traitements effectués „dans le cadre des activités d'un établissement du responsable" sur le territoire luxembourgeois[1]. La forme juridique de cet établissement, succursale ou filiale, importe peu. L'établissement exige cependant „l'exercice effectif et réel au moyen d'une installation stable"[2]. C'est dans le cadre de l'exercice des activités de cet établissement situé au Luxembourg que le traitement doit être effectué pour que les dispositions de la loi à venir puissent trouver à s'appliquer. On ne tiendra pas compte du lieu d'établissement du sous-traitant.

Si, pour reprendre l'exemple avancé par le Professeur Braibant et repris dans l'exposé des motifs[3], une entreprise française fabrique au Portugal des marchandises qu'elle vend à partir d'un établissement situé en France à des clients allemands, les traitements de données concernant le site de production seront soumis au droit portugais et les traitements se rattachant à la gestion de la clientèle allemande seront régis par le droit français, car les ventes sont le fait d'un établissement français.

Ce critère de l'établissement est clair et a le mérite d'empêcher des situations dans lesquelles un traitement pourrait être soumis à une multitude de législations applicables.

Si, par exemple, un établissement français se voit confier la gestion de données relatives à la gestion du personnel ou du stock d'établissements anglais, allemands, portugais et luxembourgeois, on évite l'application cumulative des lois française, anglaise, allemande, portugaise et luxembourgeoise à un seul traitement. En effet alors même que ce traitement unique de données „multinationales" est effectué au bénéfice de tous les établissements précités, il n'est mis en œuvre que dans le cadre des activités de l'établissement français. Il ne faut donc pas analyser qui est le bénéficiaire du traitement, mais déterminer dans le cadre des activités de quel établissement le traitement est réalisé. Dans l'exemple précité, le traitement est effectué par l'établissement français dans le cadre de ses activités. „Les autres sociétés, au profit desquelles le traitement est poursuivi, ne seraient soumises qu'à leurs lois dans la mesure où elles effectuent un nouveau traitement à l'aide des données centralisées[4]." Dans pareille situation, les autres sociétés prendraient chacune la qualité de responsable du traitement pour les traitements ultérieurs.

L'OCDE considère qu'un site web n'est pas un établissement stable. Un accord sur l'hébergement d'un tel site n'aboutit pas créer un établissement stable pour l'entreprise qui exerce ses activités par le biais de ce site. L'établissement du fournisseur de services n'est pas, en principe, à prendre en considération. Un local qui héberge des équipements informatiques peut constituer un établissement si des activités sont exercées par l'intermédiaire de ce local[5].

Sont aussi visés les traitements effectués par un responsable du traitement établi en un lieu où, conformément aux règles du droit international public, est applicable le droit luxembourgeois.

2. Les moyens de traitement établis sur le territoire luxembourgeois (article 3, paragraphe (1) lettre (b))

Ce n'est pas parce que le responsable du traitement n'est pas établi sur le territoire luxembourgeois ou en un lieu où le droit luxembourgeois est applicable, que le projet de loi n'a pas vocation à s'appliquer.

Si le responsable du traitement n'est pas établi au Luxembourg ni dans un autre Etat membre de l'Union européenne, la loi luxembourgeoise s'applique à ce traitement si ce responsable utilise des

---

1 Directive, article 4, paragraphe 1, lettre a)

2 Directive, considérant 19

3 Doc. parl. 4735, p. 29

4 Léonard, Poullet, op. cit., p. 382

5 Verbiest, Wéry, Le droit de l'internet et de la société de l'information, Larcier 2001, pp. 393 et ss., Havelange, Lacoste, op. cit. p. 243

moyens de traitement situés sur le territoire luxembourgeois ou, bien que cela ne figure pas *expressis verbis* dans le texte, en tout autre lieu où s'applique le droit luxembourgeois.

Les moyens de traitement doivent s'entendre de manière large, c'est-à-dire tant des équipements que des moyens en personnel.

Cette disposition, protectrice des droits de la personne concernée[1], empêche le responsable du traitement d'échapper à l'emprise de la loi à venir en se délocalisant hors de l'Union européenne.

Si uniquement des moyens utilisés à des fins de transit sont situés sur le territoire luxembourgeois ou sur celui d'un autre Etat membre de l'Union européenne, le projet de loi sous rubrique ne s'applique pas à un tel traitement. Cette exception doit être interprétée restrictivement. Aucun traitement, ni aucune partie de celui-ci, ne doivent avoir lieu au Luxembourg ou sur le territoire d'un autre Etat membre au risque de voir appliquée la législation luxembourgeoise ou, le cas échéant, celle de cet autre Etat membre.

Lorsque le projet de loi s'applique et que le responsable du traitement n'est pas établi au Luxembourg, il doit désigner un représentant établi au Luxembourg qui se substitue à lui dans l'accomplissement des obligations imposées à un responsable du traitement établi au Luxembourg.

Il découlait de la proposition de texte faite par le Conseil d'Etat que cette désignation ne devait se faire que dans l'hypothèse de l'utilisation de moyens sur le territoire luxembourgeois à des fins de transit. Cette proposition aurait contrevenu aux dispositions de l'article 4, paragraphe 2., de la directive.

Cette substitution du responsable du traitement par un représentant établi au Luxembourg se fait par déclaration écrite adressée à la Commission nationale. Il va de soi que tout remplacement d'un représentant devra être déclaré à cette autorité.

Le représentant accomplit tous les actes que le responsable du traitement aurait dû accomplir s'il était établi lui-même au Luxembourg[2]. Les relations entre le responsable du traitement et son représentant peuvent être empreintes d'un lien de subordination caractéristique d'un contrat de travail ou, au contraire, d'une certaine autonomie comme dans un mandat. En tout cas, cette substitution ne dégage pas le responsable du traitement de sa propre responsabilité. Toute clause contraire serait nulle et non avenue.

Pour ce qui est de données collectées au Luxembourg[3] et transférées hors de l'Union européenne, nous renvoyons au point VII. ci-après.

*

II. LES CONDITIONS DU TRAITEMENT

Le projet de loi prévoit en premier lieu des conditions générales pour effectuer un traitement (A.). Eu égard à certaines catégories particulières de données ou certains traitements spécifiques, des conditions supplémentaires ont été imposées (B.).

A. Le principe de la finalité du traitement

„Un traitement d'informations nominatives est créé pour atteindre un certain but. Il doit être adapté et ne pas servir à d'autres fins. Ce principe de finalité est omniprésent."[4] Le principe de la finalité a une portée double: d'un côté les données doivent être traitées loyalement et licitement (article 4) (1.) et le traitement ne peut être effectué que s'il est légitime (article 5) (2.). En d'autres termes, l'article 5 répond à la question de savoir quand un traitement peut être mis en œuvre, l'article 4 à celle de savoir comment effectuer un tel traitement.

Le lien entre les deux dispositions est évident. Ce n'est pas parce que les données sont traitées conformément aux dispositions de l'article 4 que le traitement est automatiquement légitime ou légi-

---

1 Directive, considérant 20

2 Dans la suite du texte du projet de loi, toute référence au responsable du traitement s'applique mutatis mutandis à son représentant

3 Rappelons que la collecte fait partie intégrante de la notion de traitement

4 CNIL, Dix ans d'informatique et libertés, op. cit., p. 81

timé. Ce n'est pas parce que le traitement est légitime au regard de l'article 5 que, de ce simple fait, le responsable du traitement peut s'affranchir de respecter les règles édictées par l'article 4.

1. La qualité des données

Les données doivent être traitées loyalement et licitement. Le responsable du traitement doit s'en assurer, et non plus comme indiqué dans la version initiale, le garantir.

Le traitement loyal et licite implique „notamment" quatre conséquences, mentionnées à l'article 4, paragraphe (1)[1]. Il s'agit d'une énumération non limitative.

a. Les données doivent être collectées pour „des finalités déterminées, explicites et légitimes". Elles ne doivent pas être „traitées ultérieurement de manière incompatible avec ces finalités".

   La finalité doit être déterminée et explicite lors de la collecte[2]. Il s'agit d'un élément indispensable pour que la personne concernée puisse donner son consentement libre, spécifique et informé. La finalité doit être transparente. La personne concernée doit savoir à quoi serviront ses données.

   Il est difficile de circonscrire la notion de finalité, ce qui explique l'absence de définition dans la directive et dans le projet de loi. Cependant „il ne peut (…) être question d'englober dans une finalité un ensemble d'objectifs flous et trop nombreux"[3].

   Sous l'empire de la législation belge datant d'avant la transposition de la directive, la jurisprudence avait précisé que „doit faire l'objet d'une transparence chaque traitement, c'est-à-dire tout ensemble d'opérations marquées par une finalité unique telle que la personne concernée puisse raisonnablement, à la lecture de l'énoncé de cette finalité, concevoir les types d'opérations couvertes par cette finalité"[4].

   Il convient cependant de relever que dans bien des cas un seul traitement peut poursuivre plusieurs finalités.

   Pour qu'un seul traitement puisse poursuivre plusieurs finalités, les principes dégagés aux articles 4 et 5 du projet de loi doivent rester inchangés. Si l'un ou l'autre des ces principes se trouve modifié au regard d'une seconde finalité que le responsable du traitement entend réaliser, un nouveau traitement, avec toutes les conséquences que cela implique (par exemple: nouvelle notification à, ou autorisation de, la Commission nationale) doit être effectué. Ainsi verrons-nous plus loin que les données doivent être „adéquates, pertinentes et non excessives" au regard des finalités. Si un responsable du traitement envisage une première finalité nécessitant le traitement d'un certain nombre de données et une seconde finalité qui ne requiert le traitement que de certaines de ces données, il devra effectuer deux traitements différents, car le traitement de toutes les données sera certes proportionné au regard de la première finalité, mais ne le sera plus pour poursuivre la seconde finalité.

   C'est aussi le principe de transparence qui explique pourquoi un traitement ultérieur doit être compatible avec la ou les finalités communiquées à la personne concernée lors de la collecte.

   L'article 4, paragraphe 1er, de la loi belge du 11 décembre 1998 précise que la compatibilité doit tenir compte „notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables". La doctrine a critiqué une compatibilité automatique en cas de changement de finalité dû à une modification légale ou réglementaire[5]. Le présent projet de loi ne saurait être interprété comme permettant une telle compatibilité automatique en cas de changement de l'environnement légal ou réglementaire. Cependant il ne saurait être exclu que, dans une situation particulière, un tel changement puisse être considéré comme compatible avec la finalité initiale, sans qu'il y ait automatisme.

   Avant tout traitement ultérieur qui ne serait pas compatible avec la finalité déjà communiquée, le responsable du traitement devra en informer la personne concernée et recueillir son consentement, à moins naturellement qu'il puisse justifier le traitement par l'un des autres critères mentionnés à

---

1 Relevons que la directive fait figurer le traitement loyal et licite comme une des cinq conséquences du principe de la qualité des données, alors que le projet de loi pose le traitement loyal et licite comme principe et en fait découler les 4 conséquences qui sont reprises de la directive. Cette différence ne prête à aucune conséquence.

2 Directive, considérant 28

3 Pipers, Le respect de la vie privée, cité in doc. parl. 4735, p. 30

4 Buyle, Lanoye, Poullet, Willems, Chronique de jurisprudence „informatique", JT 1996, No 65, p. 233

5 Léonard, Poullet, op. cit., p. 385

l'article 5, paragraphe (1). Afin d'éviter que le responsable du traitement puisse être amené à réduire le droit d'information de la personne concernée à sa portion congrue, la compatibilité d'un traitement ultérieur avec la finalité initiale doit être examinée avec circonspection.

Le projet de loi prévoit un régime à part pour une catégorie déterminée de traitements ultérieurs, à savoir les traitements ultérieurs à des fins historiques, statistiques ou scientifiques. L'article 4, paragraphe (2), précise que des données traitées pour une finalité déterminée peuvent faire l'objet d'un traitement ultérieur, mais uniquement à des fins historiques, statistiques ou scientifiques. Un tel traitement ultérieur doit être préalablement autorisé par la Commission nationale qui vérifiera si ce traitement ne peut être effectué sur base de données rendues anonymes[1], c'est-à-dire ne permettant plus d'identifier la ou les personnes concernées.

b. Les données doivent être „adéquates, pertinentes et non excessives au regard des finalités" de la collecte.

Il s'agit là du principe de proportionnalité. Le responsable du traitement devra, avant de commencer un traitement, s'interroger sur les catégories de données à collecter pour pouvoir atteindre les finalités qu'il s'est fixées. La collecte des données ne doit pas aller au-delà de ce qui est nécessaire au regard de la ou des finalités poursuivies.

Ainsi, par exemple, viole ce principe de proportionnalité une banque qui „ne s'est pas contentée de cibler sa clientèle sur base de données recueillies dans le cadre de la gestion des comptes afin de lui vendre un produit; [qu'] à l'occasion de cette campagne, elle a recherché et collecté de nouvelles données relatives à l'état du portefeuille clients ayant un prêt logement à l'OCCH", en l'espèce d'un concurrent dont la banque en question s'était portée acquéreur[2]. Le traitement d'informations n'ayant aucun lien avec une finalité déterminée est à considérer comme excessif et contraire au principe de proportionnalité.

c. Les données doivent être „exactes et, si nécessaire, mises à jour".

Cette précision s'impose d'elle-même. Elle figure également à l'article 28, paragraphe (5).

Le projet de loi oblige le responsable du traitement de prendre „toute mesure raisonnable" pour que des données inexactes ou incomplètes au regard des finalités soient effacées ou rectifiées. Cette obligation de diligence s'apprécie en fonction du bon père de famille que doit être le responsable du traitement et en fonction de la finalité poursuivie par le traitement.

d. Les données doivent être „conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités" poursuivies.

Dans la mesure où seules les données „adéquates, pertinentes et non excessives" doivent être traitées, la durée de leur conservation doit également être proportionnée à la réalisation de la finalité poursuivie. Dès que les données ne sont plus nécessaires, elles doivent être effacées, sans préjudice de la possibilité d'un traitement ultérieur à des fins historiques, statistiques ou scientifiques en application des conditions posées à l'article 4, paragraphe (2).

2. La légitimité du traitement

Un traitement peut être effectué dans l'une des six hypothèses de l'article 5, paragraphe (1). Cette énumération est limitative. L'illégitimité peut également survenir en cours de traitement dès lors que le traitement ne se situe plus dans le cadre tracé par l'une des ces hypothèses.

a. „Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis."

Sont par exemple visées les communications des données concernant le personnel, effectuées par une société aux organismes de sécurité social.

b. „Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées."

---

1 Article 14, paragraphe (1), lettre (b)

2 Comm. Bruxelles, 15 septembre 1994, cité in Buyle, Lanoye, Poullet, Willems, op. cit. No 72, p. 236

Cette disposition concerne le secteur public. La notion de „secteur public“ doit être interprétée de manière extensive en ce que les chambres professionnelles, pour ne citer qu'elles, doivent y être comprises.

Pour que cette disposition s'applique, soit le responsable du traitement soit le tiers auquel les données ont été communiquées doivent relever du secteur public.

L'article 5, paragraphe (1) lettre (b), ne doit pas cacher l'existence d'une autre contrainte s'appliquant en la matière. Il faut en effet respecter les exigences posées à l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme[1] qui prévoit que „il ne peut y avoir ingérence d'une autorité publique dans l'exercice [du droit au respect de la vie privée et familiale] que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui“.

c. „Le traitement 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.“

L'exécution du contrat ou l'exécution réclamée par la personne concernée d'une mesure précontractuelle est dans l'intérêt de la personne concernée, puisque celle-ci a consenti au contrat et à son exécution ou a demandé l'exécution d'une mesure précontractuelle. Ce serait sinon mettre le responsable du traitement dans l'impossibilité d'exécuter sa partie du contrat. Cette légitimité se trouve dans la droite ligne du principe de l'exécution de bonne foi de toute convention figurant à l'article 1134 du Code civil.

En cas de résolution du contrat, les données collectées devront être effacées. En cas de résiliation, le traitement devra immédiatement cesser et l'effacement des données pourra s'imposer au regard des circonstances de l'espèce.

d. „Le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er.“

La disposition figurant sous la lettre (d) réitère expressis verbis l'exigence d'une balance nécessaire entre, d'un côté, les intérêts légitimes du responsable du traitement ou des tiers qui ont reçu communication des données, et, de l'autre côté, les intérêts et les droits et libertés fondamentaux de la personne concernée.

Cette balance des droits, libertés et intérêts des parties en cause est sous-jacente dans les autres hypothèses visées à l'article 5, paragraphe (1).

La lettre (d) se situe résolument dans le cadre tracé par l'article 1er du projet de loi. Le traitement est illégitime dès lors que la balance penche en défaveur de la personne concernée. Il appartient à la Commission nationale de surveiller le respect de cette balance.

Le document parlementaire 4735 énumère aux pages 31 et 32 quelques exemples illustrant le respect d'une telle balance des intérêts en cause.

Nous voudrions brièvement approfondir le deuxième exemple. Il y est précisé que „les données à caractère personnel sont traitées à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, à condition toutefois que les résultats soient publiés sous une forme ne permettant pas d'identifier les personnes concernées“.

C'est dans le cadre de cet exemple qu'il convient de considérer la situation décrite au considérant 30 de la directive. Ce considérant autorise les Etats membres „en vue d'assurer l'équilibre des intérêts en cause, tout en garantissant une concurrence effective (…) [à] préciser les conditions dans lesquelles des données à caractère personnel peuvent être utilisées et communiquées à des tiers dans le cadre d'activités légitimes de gestion courante des entreprises et autres organismes“.

---

1 Cette disposition est d'ordre public (CE 17 juillet 1992, Pas. 28, 288) et d'effet direct, c'est-à-dire qu'elle crée au profit des justiciables des droits que les juridictions nationales sont chargées de sauvegarder (Cour 13 novembre 1996, Pas. 30, 154)

Il semble par trop péremptoire que d'affirmer que les résultats des traitements de données effectués par exemple dans le cadre d'une planification ne devraient jamais permettre d'identifier les personnes concernées lorsque ces résultats sont publiés.

En effet, par exemple en vue de rationaliser une répartition intragroupe des tâches, si la société faîtière d'un groupe de sociétés, dont au moins une est établie au Luxembourg, décide de faire le relevé du personnel employé, de la description des postes occupés, du nombre de salariés ainsi que de la rémunération payée et autres avantages consentis à ces salariés, sans que ces données soient publiées ailleurs qu'au sein dudit groupe, on ne saurait douter a priori du caractère légitime d'un tel traitement. Certes des relevés globaux sont envisageables. Mais il peut exister des postes qui, par leur nature ou parce qu'ils ne sont occupés que par une seule personne[1], permettent l'identification de la personne concernée malgré l'existence de relevés globaux. En pareille circonstance, et sous réserve des circonstances de l'espèce, on peut néanmoins partir du principe de la légitimité d'un tel traitement.

Il doit en aller de même, toujours sous la même réserve que précédemment, lorsqu'une personne souhaite se porter acquéreur d'une société et, avant de signer le contrat d'achat, fait procéder à l'inventaire des actif et passif de cette société. Les données ainsi recueillies doivent pouvoir être traitées.

e. „Le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée."

f. „La personne concernée a donné son consentement."

Il est renvoyé à la page 32 du document parlementaire 4735 pour les conséquences du retrait d'un consentement.

B. Conditions spécifiques à certains traitements

1. Le traitement des données sensibles

Le traitement de données sensibles est régi par l'article 6. La structure de cet article, pour complexe qu'elle soit[2], a été reprise de la directive et est logique. Le premier paragraphe établit le principe de l'interdiction du traitement des données sensibles. Les exceptions sont prévues aux paragraphes (2) à (3). Le paragraphe (4) traite des données génétiques et le paragraphe (5) fixe les sanctions pénales.

Les traitements de données sensibles ne sont pas interdits en tant que tels. C'est uniquement lorsque le traitement de ces données révèle „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" que ce traitement tombe sous la prohibition du paragraphe (1)[3]. Elargissant le champ d'application de la directive en la matière, le projet de loi ajoute que l'interdiction s'étend au traitement des données génétiques.

La loi belge du 11 décembre 1998 dispose que les données sensibles sont celles qui „révèlent l'origine raciale ou ethnique, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la vie sexuelle".

Le projet de loi se démarque de la législation belge en ce que l'accent est mis sur le traitement des données sensibles. Ce ne sont pas les données qui révèlent leur caractère sensible, mais leur traitement. Conformément au principe de finalité, c'est la finalité qui fera que le traitement tombe ou ne tombe pas dans le champ d'application de l'article 6, paragraphe (1). En d'autres termes, si la finalité est de traiter des données pour révéler leur caractère sensible, l'interdiction trouvera application. Ce n'est donc pas parce que l'on est en présence de données sensibles que tout traitement est ipso facto interdit[4].

Par exemple, le traitement d'un chèque adressé à une organisation syndicale et portant la mention „cotisation" et le traitement par une compagnie aérienne de l'exigence pour un passager d'un repas „kasher" ne doivent pas poser de problème au regard de l'article 6[5].

---

1 Chef d'établissement, membres du conseil d'administration, gérant, mais aussi par exemple chef du personnel, conseiller juridique, portier

2 La matière à réglementer l'est d'ailleurs aussi

3 La „vie sexuelle", terme utilisé dans la directive, inclut l'orientation sexuelle

4 C'est pourquoi l'utilisation des termes „traitement de données sensibles" peut prêter à confusion. S'agissant cependant d'un terme souvent utilisé, comme c'est le cas des termes „protection des données" (voir supra), nous continuerons à les utiliser

5 On suppose que les conditions de légitimité et de qualité des données sont remplies

Si le traitement de données révélant une appartenance syndicale ou les opinions religieuses était interdit, les traitements mentionnés ci-avant seraient prohibés. Or telle n'a pas été l'orientation du projet de loi. Dans ces deux exemples précités, la finalité du traitement n'est pas axée sur la sensibilité des données.

Est par contre prohibé un traitement visant à répertorier des passagers de confession juive en fonction de l'exigence d'un repas „kasher". De même est interdit tout traitement utilisé par l'employeur pour distinguer les salariés qui sont syndiqués de ceux qui ne le sont pas.

Les données sensibles peuvent être traitées dans les hypothèses suivantes:

a. „La personne concernée a donné son consentement à un tel traitement, sauf indisponibilité du corps humain et sauf le cas interdit par la loi." (article 6, paragraphe (2) lettre (a))

b. „Le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement notamment en matière de droit du travail dans la mesure où il est autorisé par la loi." (article 6, paragraphe (2) lettre (b))

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." (article 6, paragraphe (2) lettre (c))

d. „Le traitement est mis en oeuvre, 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." (article 6, paragraphe (2) lettre (d))

e. „Le traitement porte sur des données manifestement rendues publiques par la personne concernée." (article 6, paragraphe (2) lettre (e))

f. „Le traitement mis en oeuvre conformément aux règles de procédures judiciaires en matière civile applicables est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice s'il est mis en oeuvre à cette fin exclusive." (article 6, paragraphe (2) lettre (f))

   Sont uniquement visées les procédures judiciaires en matière civile[1]. Les procédures pénales sont mentionnées à l'article 6, paragraphe (3)[2]. Ainsi, l'établissement d'une filiation par recoupement de séquences génétiques tombe sous la lettre (f) de l'article 6, paragraphe (2), alors que si des séquences génétiques servent à rechercher ou à confondre l'auteur d'un meurtre ou d'un viol, c'est l'article 6, paragraphe (3) qui s'appliquera. Comme nous le verrons au point par la suite, les paragraphes (2) lettre (f), et (3) de l'article 6 s'appliquent également au traitement des données génétiques

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 [du projet de loi] et que ce traitement est mis en oeuvre conformément au régime d'autorisation préalable de la Commission nationale tel que prévu à l'article 14 [de ce même projet de loi]." (article 6, paragraphe (2) lettre (g))

h. „Le traitement est mis en oeuvre par voie de règlement grand-ducal tel que prévu à l'article 17 [du projet de loi]." (article 6, paragraphe (2) lettre (h))

i. Le principe de l'interdiction du traitement de données sensibles „ne s'applique pas lors d'une procédure judiciaire ou d'une enquête pénale. Toutefois les données génétiques ne peuvent être traitées que 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." (article 6, paragraphe (3))

j. En vertu du paragraphe (4) de l'article 6, les données génétiques peuvent faire l'objet d'un traitement:

   – dans des cas visés par les articles 6, paragraphe (2) lettres (c) (intérêts vitaux de la personne concernée), (f) (procédures judiciaires en matière civile), (g) (motif d'intérêt public), (h) (autorisation par voie réglementaire), 6 paragraphe (3) (procédures pénales) et 7 (données traitées par les services de la santé), et

---

1 Les procédures d'arbitrages sont exclues

2 Voir point i. ci-après

– lorsque „la personne concernée a donné son consentement et si le traitement est effectué dans les seuls domaines de la santé ou de la recherche scientifique sauf indisponibilité du corps humain et 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".

k. Le traitement de certaines catégories de données par les services de la santé est régi par l'article 7.

Les conditions posées par l'article 7 sont les suivantes:

– Le traitement doit être „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, de la recherche scientifique dans le domaine de la biologie[1] et de la médecine".

– Le traitement doit être effectué par une instance médicale. L'article 2, lettre (i), définit l'instance médicale comme „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".

– Le traitement peut aussi être effectué „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 oeuvrant dans les domaines social, familial et thérapeutique désignées par règlement grand-ducal". La commission a décidé d'inclure les „entreprises d'assurance, les sociétés gérant les fonds de pension et la Caisse médico-chirurgicale mutualiste" dans les prévisions de l'article 7, paragraphe (1), sous peine de leur interdire toute activité. En revanche, afin d'éviter des abus, la commission a repris la proposition faite par le Conseil d'Etat dans son avis complémentaire de supprimer le terme trop vague de „mutuelles". Cependant la commission, tout en partageant les craintes du Conseil d'Etat à propos des personnes oeuvrant dans le domaine ASFT, a décidé de limiter les personnes autorisées à traiter des données sensibles en exigeant leur énumération limitative dans un règlement grand-ducal.

La simple collecte de données relatives à la santé tombe sous le champ de la loi et ne peut être pratiquée que par un organisme à ce autorisé à l'article 7. Or lesdits organismes ne sauraient fonctionner et verser des pensions d'invalidité sans disposer de données relatives à la santé. Dans ces situations, l'article 7 précise que le responsable du traitement doit être soumis au secret professionnel.

– Le traitement doit avoir été préalablement autorisé par la Commission nationale. Ne sont soumis qu'à notification le traitement mis en oeuvre conformément à l'article 36 de la loi du 28 août 1998 sur les établissements hospitaliers ainsi que le traitement mis en oeuvre par un médecin et concernant ses patients[2].

Un règlement grand-ducal déterminera les conditions dans lesquelles les données concernées pourront être communiquées à des tiers ou être utilisées à des fins de recherche scientifique. La communication indue à des tiers tombe sous le coup de la sanction pénale prévue à l'article 7, paragraphe (5).

2. Le traitement de données judiciaires

Les données judiciaires, c'est-à-dire les données traitées dans le cadre d'enquêtes pénales ou de procédures judiciaires civiles ou administratives ne peuvent faire l'objet d'un traitement que dans les conditions du droit commun de la procédure pénale, civile ou administrative. Les traitements de données sensibles restent régis par l'article 6 du projet de loi.

Les données relatives aux infractions, condamnations pénales ou mesures de sûreté, y compris dans le cadre de la protection de la jeunesse, doivent être traitées en exécution d'une disposition légale[3].

---

1 Y compris de la biotechnologie

2 Article 7, paragraphe (3)

3 Y compris une disposition figurant dans un règlement grand-ducal

Conformément à l'article 8, paragraphe 5., de la directive et de l'article 8, paragraphe (3) du projet de loi, le casier judiciaire reste sous le contrôle du Procureur général d'Etat, autorité publique compétente en la matière[1].

3. La liberté d'expression

Dans son avis du 29 janvier 2002, le Conseil d'Etat avait suggéré de reporter l'examen de l'article 9 de la directive lors de la discussion sur le projet de loi concernant la liberté dans les moyens de communication de masse. Il s'agissait pour le Conseil d'Etat d'une matière dans laquelle l'arbitrage entre la liberté d'expression et le droit à la vie privée est d'autant plus délicat que la marge de manœuvre des Etats membres reste importante.

La commission a cependant décidé de maintenir l'article 9 dans le projet de loi, puisque le Luxembourg se doit de transposer la directive qui précise explicitement dans son article 9 que „les Etats membres prévoient, pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations au présent chapitre, au chapitre IV et au chapitre VI dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression". L'article 9 de la directive impose aux Etats membres une obligation. Il ne s'agit pas d'une faculté. Retirer l'article 9 du projet de loi signifierait une transposition incomplète de la directive.

L'article 9 s'applique aux traitements mis en œuvre aux seules fins de journalisme ou d'expression artistique ou littéraire. La future loi sur la liberté dans les moyens de communication de masse va prévoir des dispositions particulières uniquement en cas de traitement mis en œuvre aux fins de journalisme. Ainsi, par exemple, pourra-t-elle fixer les modalités dans lesquelles seront exercés les pouvoirs de la Commission nationale. Le paragraphe (3) de l'article 9 a été supprimé, alors qu'il s'agissait d'une disposition qui ne concernait uniquement le domaine du journalisme et n'était en aucune relation avec les formes d'expression artistique ou littéraire pourtant également visées par l'article 9.

Aucune définition n'a été donnée pour les termes de „journalisme ou d'expression artistique ou littéraire". La doctrine belge privilégie un concept fonctionnel de ces notions. C'est en effet non une catégorie professionnelle que la directive, et par conséquent, le projet de loi veulent réglementer, mais certains traitements de données effectués dans le cadre du journalisme et d'une forme d'expression artistique ou littéraire[2]. Tant la directive que le projet de loi font référence au „traitement mis en œuvre aux seules fins de journalisme ou d'expression artistique ou littéraire". Par conséquent, „il s'agit d'exempter certains traitements dont la finalité est la production en vue de la communication au public d'une expression dont la prétention esthétique, intellectuelle ou d'information sur l'actualité est affirmée. A ce propos, le responsable du traitement ne sera pas forcément un journaliste, un écrivain ou un artiste mais l'organe de presse, l'éditeur, etc."[3].

Quelles sont les dispositions du présent projet de loi auxquelles il a été dérogé?

D'abord, en application de l'article 9, paragraphe (1) lettre (a), le traitement n'est pas soumis à la prohibition de traiter les données sensibles prévue à l'article 6, paragraphe (1) ni aux dispositions de l'article 8 „lorsque le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou à des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée". Par exemple, l'appartenance d'un ministre, d'un député ou d'un candidat à une élection à un parti politique déterminé tombe manifestement sous l'emprise de cette disposition.

Ensuite, un transfert de données vers un pays tiers peut avoir lieu, nonobstant le fait que ce pays tiers n'offre pas le niveau de protection adéquate exigé par l'article 18, paragraphe (1).

Puis l'article 9, paragraphe (1) lettre (c), dispose que l'obligation d'information de l'article 26, paragraphe (1), n'est pas applicable „lorsque son application compromettrait la collecte des données auprès de la personne concernée".

De même, en vertu de la lettre (d), il est dérogé à l'obligation d'information visée à l'article 26, paragraphe (2), „lorsque son application compromettrait soit la collecte des données, soit une publication en

---

1 Article 1er du règlement grand-ducal modifié du 14 décembre 1976 portant réorganisation du casier judiciaire

2 Léonard, Poullet, op. cit., p. 381

3 Ibid. eod. loc.

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".

Enfin, l'article 9, paragraphe (1) lettre (e), aménage le droit d'accès de la personne concernée „qui peut être différé ou limité conformément à l'article 28, paragraphe (4) et à l'article 29". Il s'agit ici d'une dérogation facultative. L'article 29, paragraphe (1) lettre (g), du projet de loi permet au responsable du traitement de limiter ou de différer l'accès aux données, de même qu'aux informations sur leur origine, en se prévalant de la liberté d'expression. Le droit d'accès de la personne concernée „peut être différé ou limité", mais ne doit pas l'être. La décision incombera au responsable du traitement qui devra apprécier l'opportunité de cette dérogation. En vertu de l'article 28, paragraphe (4), si le droit d'accès a été refusé et si les données en cause n'ont pas encore été publiées, la personne concernée devra demander à la Commission nationale d'avoir accès à ces données ainsi qu'aux informations disponibles sur leur origine. Cependant le responsable du traitement pourra toujours arguer du secret de ses sources pour refuser la divulgation des origines.

En revanche, même dans le cadre d'un traitement aux seules fins de journalisme ou d'expression artistique ou littéraire, le responsable du traitement devra s'assurer que les autres dispositions du projet de loi, comme par exemple, les conditions de légitimité et de qualité des données prescrites aux articles 4 et 5 sont respectées. L'article 9 n'implique en effet aucune dérogation générale aux dispositions du projet de loi, mais seulement des dérogations spécifiques et limitativement énumérées.

Du point de vue des procédures administratives, le contenu d'une notification est limité aux seuls nom et adresse du responsable du traitement.

4. Les traitements à des fins de surveillance

La surveillance consiste en „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"[1].

Le projet de loi détermine les règles applicables à toute forme de surveillance (a.) tout en soumettant la surveillance sur le lieu du travail à un régime particulier (b.).

Il se peut qu'un même traitement tombe dans le champ d'application soit de l'article 10 soit de l'article 11 en fonction de la personne concernée. Par exemple, une caméra dans une grande surface tombe sous le coup de l'article 10 si la personne concernée est un client, même potentiel, du magasin et sous celui de l'article 11 si la personne concernée est un salarié employé par le propriétaire de ce magasin.

Quel que soit le régime applicable, la ratio legis exige que les moyens de surveillance ne soient pas cachés (principe de la transparence).

a. *Le régime général*

Depuis quelques années, le nombre de caméras et autres moyens de surveillance dans des lieux tant privés que publics augmente considérablement. Ainsi, par exemple, un habitant de Londres est susceptible d'être filmé en moyenne 300 fois chaque jour par une des nombreuses caméras de surveillance[2]. Afin d'éviter de dégénérer de la société de l'information – concept empreint de liberté – en société du contrôle de l'information, une intervention du législateur s'impose.

La surveillance doit être effectuée conformément aux dispositions de l'article 4 du projet de loi.

Dérogeant à l'article 5, les hypothèses dans lesquelles une surveillance peut être effectuée sont au nombre de trois:

– si la personne concernée y a consenti;
– „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."

1 Article 2, lettre (q)

2 Focus, 15/2002

Le texte initial du projet de loi ne visait que la finalité de la prévention, la recherche, la constatation et la poursuite d'infractions pénales. D'après l'article 17 du projet de loi, les traitements nécessaires à cette finalité sont autorisés par voie réglementaire. Le Conseil d'Etat a donc suggéré de remplacer cette finalité par la „sécurité des usagers" et „la prévention des accidents" au motif qu'il fallait prévenir toute insécurité juridique en distinguant les champ d'application respectifs des articles 10 et 17. La commission s'est ralliée à cette manière de voir.

Le texte de l'article 10, paragraphe (1) lettre (b), répond à cette préoccupation. Cependant il serait inexact de faire abstraction de la finalité consistant en la prévention, la recherche, la constatation et la poursuite d'infractions pénales. „Les données recueillies au cours [du traitement à des fins de surveillance] sont donc susceptibles d'un traitement ultérieur dans le cadre général de la politique pénale, mais ne le sont pas nécessairement."[1] Le projet de loi prévoit d'ailleurs expressément au paragraphe (3) lettres (b) et (c) de l'article 10 que les données collectées dans le cadre d'une activité de surveillance peuvent être communiquées aux autorités publiques agissant dans le cadre de l'article 17, c'est-à-dire que dans le cadre de la prévention, la recherche et la constatation d'infractions pénales, ainsi qu'aux autorités compétentes pour constater ou poursuivre une infraction pénale. La „sécurité des usagers" ou la „prévention des accidents" incluent donc la prévention, la recherche, la constatation et la poursuite d'infractions pénales, puisqu'un traitement ultérieur à ces fins est prévu dans le projet de loi.

Ainsi, par exemple, un responsable du traitement peut installer une caméra près d'un distributeur automatique de billets de banque. La finalité de cette surveillance est la sécurité des usagers. Les données recueilles par ce biais pourront toujours être communiquées aux autorités chargées de la prévention, la recherche, la constatation et la poursuite d'infractions pénales.

Sont visés tous les lieux accessibles ou non au public, y compris les bâtiments publics et administratifs, mais à l'exception des lieux d'habitation. Les lieux d'accès privé, parmi lesquels peuvent être rangés les lieux d'habitation sont mentionnés à la lettre (c) de l'article 10, paragraphe (1). La commission n'a donc pas repris la proposition de supprimer la référence aux locaux d'habitation faite par le Conseil d'Etat dans son avis complémentaire du 2 juillet 2002.

– „aux lieux d'accès privé dont la personne physique ou morale y domiciliée est le responsable du traitement." Pour ce qui est des personnes morales, doivent être visés non seulement le siège social, mais aussi le siège des succursales et des établissements.

  Le champ de vision des caméras servant à surveiller un tel lieu d'accès privé doit naturellement être limité afin de ne pas déborder sur un lieu d'accès public, comme un trottoir ou la voie publique.

En vertu de l'article 10, paragraphe (2), l'information de la personne concernée se fait par le biais de panneaux de signalisation, de circulaires, d'envois recommandés par voie postale ou électronique ou par tout autre moyen approprié. Cette information doit être soit préalable soit concomitante au traitement. Elle s'étend aux abords ou dans tout lieu visé à la lettre (b) du paragraphe (1) et aux lieux d'accès privé de la lettre (c) de ce paragraphe. Si le responsable du traitement entend soumettre l'entrée de son domicile à une surveillance par caméra, il faut qu'il en informe tout visiteur. Il est évident qu'aucune information préalable ou concomitante n'est requise en cas de consentement de la personne concernée.

Pour des raisons pratiques évidentes, l'information de la personne concernée est limitée à l'existence d'une surveillance. Cependant la personne concernée peut demander au responsable du traitement toutes les informations figurant au paragraphe (2) de l'article 26, comme notamment l'identité du responsable du traitement et, le cas échéant, de son représentant, la ou les finalités déterminées du traitement auquel les données sont destinées, les catégories de données concernées ou la durée de conservation des données. L'exigence que ces informations figurent à côté ou en dessous d'une caméra de surveillance aurait été totalement disproportionnée. Si la personne concernée souhaite s'enquérir, par exemple, de la finalité du traitement, une démarche active de sa part sera nécessaire.

Conformément au paragraphe (3), la communication des données recueillies peut avoir lieu:

– à tout tiers si la personne concernée a donné son consentement sauf lorsqu'une telle communication est interdite par la loi;
– aux autorités publiques agissant dans le cadre de l'article 17, paragraphe (1);

---

1 Avis du Conseil d'Etat, doc. parl. 4735[6]

– 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. „Les données collectées à des fins de surveillance peuvent être communiquées à toutes les autorités judiciaires et pas seulement aux autorités pénales.“[1]

b. *La surveillance sur le lieu du travail*

L'article 11 précise les conditions dans lesquelles peut être effectué un traitement aux fins de surveillance sur le lieu du travail. Il n'a pas vocation à se substituer au droit du travail qui reste applicable pour tous les aspects qui ne sont pas abordés par cet article ou, par extension, par le présent projet de loi[2].

La première question qui s'est posée est celle de savoir si l'on devait inclure dans le projet de loi une disposition réglementant la surveillance sur le lieu du travail.

Les chambres professionnelles étaient partagées. La Chambre de Travail s'y opposait catégoriquement, la Chambre des Fonctionnaires et Employés Publics soulevait des problèmes d'applicabilité à la fonction publique, la Chambre des Métiers accueillait favorablement le principe d'une réglementation, alors que la position de la Chambre des Employés Privés était plus nuancée[3].

Dans son avis du 29 janvier 2002, le Conseil d'Etat a suggéré de supprimer l'article 11 et d'approfondir la problématique en la plaçant dans un contexte plus général.

La commission du travail et de l'emploi est convaincue de la nécessité de légiférer en la matière „avec la finalité d'instituer une protection efficace du salarié lui conférant toutes les garanties nécessaires pour faire respecter ses droits dans ce domaine“[4]. La commission partage cette approche en y ajoutant qu'il convient de préciser les droits et obligations tant des salariés que des employeurs.

L'article 11 intervient afin d'éviter des abus et un certain flou juridique préjudiciable pour tous.

Ceci d'autant plus que la jurisprudence de la Cour européenne des droits de l'homme n'a pas limité le droit au respect de la vie privée au seul domicile privé. „Le respect de la vie privée doit aussi englober dans une certaine mesure le droit de l'individu de nouer et de développer des relations avec ses semblables. Il n'y a aucune raison de principe d'en exclure les activités professionnelles ou commerciales.“[5]

La question de la surveillance des salariés sur le lieu du travail n'est pas nouvelle.

Déjà en 1938, la cour d'appel de Paris a condamné le directeur d'un journal pour avoir ouvert des lettres adressées à l'attention personnelle d'un rédacteur[6].

La jurisprudence française a déjà eu l'occasion de se prononcer sur l'utilisation par le salarié pendant les heures de travail de moyens de télécommunications appartenant à l'employeur. Cette jurisprudence s'est développée dans le cadre de litiges intervenus suite au licenciement du salarié qui avait utilisé le téléphone, le minitel ou l'ordinateur mis à sa disposition par l'employeur pour vaquer à ses tâches professionnelles, mais „détournés“ par lui à des fins privées.

Outre le caractère particulier de chaque cas d'espèce, lié à l'appréciation souveraine des circonstances de fait, le débat s'est surtout concentré sur le caractère licite des preuves apportées par l'employeur. „Si l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps du travail, tout enregistrement, quels qu'en soient les motifs, d'images ou de paroles à leur insu,

---

1 Conseil d'Etat, avis complémentaire, sub Article 10, dernier alinéa

2 Comme, par exemple, pour la définition du lieu du travail

3 Pour les détails, il est renvoyé aux documents parlementaires afférents. L'avis de la commission du travail et de l'emploi (doc. parl. 4735[7]) fait un résumé des positions des chambres professionnelles

4 Doc. parl. 4735[7] p. 3

5 Arrêt du 23 novembre 1992 Niemietz/Allemagne, A 251/B, voir aussi arrêt du 27 mai 1997 Halford/Royaume-Uni. Dans cette dernière affaire, la Cour européenne des droits de l'homme a jugé que les interceptions de conversations téléphoniques de Madame Halford faites à partir de son lieu de travail constituaient une violation de l'article 8 CEDH. Certains commentateurs ont estimé au regard des circonstances de l'affaire Halford (Madame Halford n'avait pas été informée au préalable de la possibilité pour l'employeur d'intercepter les conversations téléphoniques et aucune restriction sur l'utilisation des téléphones n'avait été édictée) qu'il n'y aurait pas de violation de l'article 8 CEDH si le salarié avait été informé au préalable des possibilités d'interception

6 DH 1938, p. 520, voir aussi Cass. crim. 16 janvier 1992, G. P. 1992, p. 296

constitue un mode de preuve illicite."[1] L'information préalable des salariés sur l'existence de contrôles inopinés ou de moyens de surveillance légitime rend licite le moyen de la preuve. La licéité du moyen de surveillance ne préjuge pas de sa fiabilité[2].

Dans une affaire récente, la Cour de cassation française a jugé que „le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée; (…) qu'un employeur ne peut dès lors, sans violation de cette liberté fondamentale [qu'est le secret des correspondances], prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur"[3].

„La Cour de cassation (…) a manifestement entendu préserver un certain espace d'intimité au salarié, sur les lieux mêmes de son travail, dans lequel, pour reprendre les termes des conclusions de l'avocat général, le „citoyen-salarié" se substitue au „salarié-citoyen"."[4] Mais tout compte fait, ne s'agit-il pas ici d'une question de preuve illicite? L'employeur ayant administré la preuve de la faute commise par le salarié par des moyens dissimulés cachés au salarié viole lui-même le principe de loyauté exigé par l'article 1134 du Code civil.

Quoi qu'il en soit, les risques d'abus existent. Pour les salariés qui sont détournés de leurs tâches professionnelles suite à une utilisation inconsidérée d'internet ou à un envoi de messages électroniques, avec les dangers inhérents à ces moyens de communication (virus, encombrement des réseaux, blocage de mémoire de l'ordinateur, consultation de sites à caractère pornographique ou pédophile). L'employeur peut, par le biais de traces laissées par l'employé (cookies, disque dur, relevés téléphoniques[5], caméras cachées), pénétrer la sphère intime du salarié.

On a parlé à ce sujet d'„éthique de la preuve"[6] ou de „morale de la preuve"[7].

Ces constatations renforcent la nécessité de légiférer en la matière. Une balance entre les différents intérêts doit être trouvée[8]. Une confiance réciproque doit s'installer entre employeur et salariés.

L'article 11 n'est pas le seul instrument juridique pouvant être invoqué en la matière. On peut citer, sans vouloir être exhaustif, l'article 8 de la Convention européenne des droits de l'homme sur le respect de la vie privée et familiale, l'article 28 de la Constitution sur le secret des lettres, la loi du 11 août 1982 concernant la protection de la vie privée et la recommandation R (89) 2 du 18 janvier 1989 du comité des ministres du Conseil de l'Europe sur la protection des données à caractère personnel utilisées à des fins d'emploi. On peut également soulever l'existence d'un recueil de directives pratiques adopté par le Bureau International du Travail le 7 octobre 1996[9].

Cet article 11 se base sur une convention collective belge No 68 adoptée le 16 juin 1998 „relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail". Le champ d'application de l'article 11 s'étend quant à lui à tout mode de surveillance et pas seulement celui par caméras.

En vertu de l'article 11, un traitement à des fins de surveillance sur le lieu du travail est soumis aux conditions suivantes[10]:

---

1 Cass. soc. 20 novembre 1991, D.1992, p. 73. La chambre criminelle de la Cour de cassation française a cependant admis des documents obtenus „dans des conditions douteuses" à titre d'indices dès lors qu'il y a eu débat contradictoire à leur sujet (sur ce dernier point: Gautier, D. 2001, p. 3152, No 11)

2 Colonna, JCP 1995, II, 22514

3 Cass. soc. 2 octobre 2001, D. 2001, p. 3148

4 Weiss, D. 2001, IR, p. 2944

5 Pour les tribunaux français, même en l'absence d'information préalable des salariés, l'employeur est en droit d'administrer la preuve d'un usage important du téléphone à des fins privées par le biais de la facturation détaillée établie par l'opérateur de téléphone (Cass. soc. 11 mars 1998, cité in Bossu, Nouvelles technologies et surveillance du salarié, RJS 2001, p. 665)

6 Chauvy, conclusions sous Cass. soc. 20 novembre 1991, précité

7 Denis, Quelques aspects de l'évolution récente du système des preuves en droit civil, RTDciv. 1977, p. 673

8 Aux Etats-Unis, cette balance penche, pourrait-on en douter?, nettement en faveur de l'employeur. (Waldmeir, US employees find no right to privacy in cyberspace, www.FT.com du 12 août 2001)

9 Pour un résumé de ce recueil: CNIL, La cybersurveillance des salariés dans l'entreprise, mars 2001, p. 19

10 Nous n'aborderons pas une nouvelle fois l'exigence que le traitement soit adéquat, pertinent et non excessif au regard de la finalité recherchée. Le principe de la qualité des données de l'article 4 s'applique également aux traitements à des fins de surveillance sur le lieu de travail

– l'employeur doit être le responsable du traitement;
– le traitement doit avoir été préalablement autorisé par la Commission nationale;
– le traitement doit être nécessaire pour poursuivre l'une des finalités suivantes:

(a) les besoins de sécurité et de santé des travailleurs,

(b) les besoins de protection des biens de l'entreprise,

Sont visées en première ligne les caméras installées aux entrées et sorties de l'établissement, y compris les entrées du personnel. Relèvent également de la protection des biens de l'entreprise les moyens de surveillance destinés à s'assurer que des virus ne pénètrent pas le réseau d'ordinateurs, que des fichiers professionnels ne soient pas détruits, que le réseau ne soit pas encombré. On peut encore y ajouter les écoutes téléphoniques effectuées par des établissements de crédit et autres professionnels du secteur financier aux fins d'enregistrer les ordres des clients passés par téléphone à condition toutefois que tant le client ait donné son accord à un tel enregistrement et que le salarié ait été informé que les conversations téléphoniques passées par ce téléphone seront enregistrées.

(c) le contrôle du processus de production portant uniquement sur les machines,

La convention collective belge No 68 précise à ce sujet que „si le contrôle porte uniquement sur les machines, il a pour but d'en vérifier le bon fonctionnement"[1]. Ainsi l'accès par un technicien aux ordinateurs des salariés a-t-il pour but d'assurer le bon fonctionnement du système.

(d) le contrôle temporaire de production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte.

Il ne doit y avoir aucun autre moyen pour déterminer la rémunération exacte du salarié, par exemple en cas de travail à la tâche. Le projet de loi est à cet égard plus restrictif que la convention collective dont il s'inspire. En outre il ne peut s'agir que d'un contrôle temporaire.

(e) dans le cadre d'une organisation de travail selon l'horaire mobile conformément à la loi.

Il s'agit de tenir compte des spécificités de la loi „PAN" et des dispositions applicables à la fonction publique.

Les finalités étant limitativement énumérées, l'employeur ne saurait détourner les données recueillies pour une autre finalité incompatible avec celle qu'il entendait poursuivre initialement et qu'il a communiquée aux parties concernées en application de l'article 11, paragraphe (2).

Est-ce que l'employeur peut utiliser les données recueillies dans le cadre d'un traitement légitime sur le lieu du travail à l'appui d'un licenciement?

Dès lors que les données ne sont pas détournées de leur finalité, elles peuvent être utilisées en justice. Si, par exemple, des moyens de surveillance ont été installés en vue de la protection des biens de l'entreprise et qu'il appert des données qu'un salarié a porté atteinte à la propriété de l'entreprise en commettant, par exemple, un vol, la finalité n'a pas été détournée. Cette réponse ne concerne que la loyauté de la preuve et non sa fiabilité ou sa pertinence.

Dans les cas visés aux lettres (a), (d) et (e) de l'article 11, paragraphe (1), le comité mixte d'entreprise, s'il y en a un, a un pouvoir de décision tel que défini à l'article 7 paragraphes (1) et (2) de la loi modifiée du 6 mai 1974 instituant des comités mixtes dans les entreprises du secteur privé et organisant la représentation des salariés dans les sociétés anonymes. La commission du travail et de l'emploi relève, à juste titre, que les autres finalités ne rentrent pas dans le domaine de compétence du comité mixte d'entreprise. Il a été décidé de ne pas modifier la loi du 6 mai 1974 en vue d'étendre le domaine de cogestion pour les raisons évoquées dans l'avis de la commission du travail et de l'emploi[2]. En outre les matières visées aux lettres (b) et (c) relèvent de la responsabilité de l'employeur qui doit garder le pouvoir de décision sur l'organisation de l'entreprise.

En raison du lien de subordination entre l'employeur et le salarié – personne concernée, l'article 11 précise que le consentement de ce dernier ne rend pas légitime le traitement mis en oeuvre par l'employeur.

---

1 Article 4 de la convention collective. A noter que celle-ci s'applique également au contrôle du processus de production portant sur les travailleurs

2 Doc. parl. 4735[7], p. 4

Suivant en cela les principes dégagés par la jurisprudence française sur la loyauté des modes de preuves, le paragraphe (2) de l'article 11 dispose que doivent être 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; et
– 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.

L'article 32, paragraphe (6) indique que la personne concernée ainsi que les organes précités peuvent saisir la Commission nationale s'ils estiment que l'employeur n'a pas respecté les dispositions de l'article 11. En raison de la sensibilité de cette matière, qui pourrait envenimer la situation au sein de l'entreprise, la Commission nationale doit statuer dans le mois de sa saisine. L'action en cassation leur est aussi ouverte dans les conditions de l'article 39. Mais, pour les raisons avancées par le Conseil d'Etat dans son avis complémentaire du 2 juillet 2002, l'inopposabilité à la Commission nationale du secret professionnel auquel le responsable du traitement est astreint n'a pas été étendue à la la Commission nationale saisie en vertu de l'article 32, paragraphe (6).

Pour terminer, il convient de signaler l'existence d'un document travail adopté le 29 mai 2002 par le groupe institué par l'article 29 de la directive[1]. Il s'agit là d'un document important qui synthétise les réflexions de ce groupe de travail sur la surveillance des modes électroniques de communication, courriers électroniques et internet, sur le lieu de travail.

Ce document de travail[2] énumère les conditions dans lesquelles l'employeur peut procéder à la surveillance des courriers électroniques et d'internet sur le lieu du travail.

Avant de commencer toute surveillance, l'employeur doit s'assurer que cette surveillance est absolument nécessaire pour une finalité déterminée. Cette surveillance ne doit pas être continue et ne doit être envisagée que dans des circonstances exceptionnelles, comme par exemple, lorsque l'employeur doit protéger ses intérêts en cas d'activité criminelle développée par le salarié, ou pour assurer la sécurité du système (détection de virus).

L'activité de surveillance doit être gouvernée par la transparence, tant à l'égard des autorités[3] et des salariés, voire même à l'égard des tierces personnes[4]. L'information des salariés doit être claire, précise et exacte[5]. Les circonstances dans lesquelles la surveillance a lieu doivent être décrites avec précision, comme par exemple, les conditions dans lesquelles le matériel de l'entreprise peut être utilisé à des fins privées, les conditions de la surveillances (par qui, quand, comment), les conséquences qui pourraient être tirées des résultats de cette surveillance.

Le groupe de travail estime recommandé pour l'employeur d'informer immédiatement le salarié d'un usage non autorisé des moyens de télécommunications et notamment d'internet[6].

L'employeur ne saurait poursuivre des traitements illégitimes et surveiller des activités ayant trait à des données sensibles du salarié.

La surveillance doit être adaptée au but légitime poursuivi. L'employeur doit recourir aux moyens de surveillance les plus protecteurs de la sphère privée du salarié. Le respect de ce principe de proportionnalité exige que, par exemple, doivent être évitées les surveillances automatiques et continues des salariés. De même la surveillance du contenu des courriers électroniques peut être disproportionnée, alors que l'employeur peut se limiter à surveiller les temps d'utilisations, le nombre de courriers électroniques ou la taille des annexes.

---

1 Les missions de ce groupe sont énumérées à l'article 30 de la directive et à l'article 14 de la directive 97/66/CE. Pour un aperçu de ses activités: voir son 5ème rapport annuel (année 2000) adopté le 6 mars 2002: www.europa.eu.int/comm/internal_market/fr/dataprot/wpdocs/index.htm

2 Dont seulement une version anglaise est disponible sur le site internet précité

3 L'article 11 exige d'ailleurs une autorisation préalable de la Commission nationale

4 Par exemple, indication standard sur un courrier électronique adressé à une personne extérieure à l'entreprise que la réponse peut faire l'objet d'une mesure de surveillance

5 On peut par exemple penser par une stipulation insérée dans le contrat de travail

6 Par un message d'alerte qui s'affiche sur l'écran d'ordinateur

Des techniques permettent de limiter ou de bloquer l'accès à internet[1]. L'employeur doit également agir avec discernement et tenir compte des possibilités de réponses erronées de moteurs de recherche, de liens erronés ou de publicités trompeuses.

*

III. LES DROITS DE LA PERSONNE CONCERNEE

Le chapitre VI du projet de loi traite des droits de la personne concernée. Il s'agit du droit à l'information (A.), du droit d'accès (B.) et du droit d'opposition (C.), lequel n'était pas prévu dans la législation antérieure. S'ajoute encore la question des décisions individuelles automatisées (C.).

A. Le droit à l'information

„Le traitement loyal des données suppose que les personnes concernées puissent connaître l'existence des traitements et bénéficier, lorsque des données sont collectées auprès d'elles, d'une information effective et complète au regard des circonstances de cette collecte[2].“

1. Principe

Deux modalités d'information de la personne concernée sont visées aux articles 10 et 11 de la directive et reprises presque textuellement respectivement aux paragraphes (1) et (2) de l'article 26.

D'abord, lorsque des données sont collectées directement auprès de la personne concernée, le responsable du traitement doit fournir à celle-ci 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 autre information supplémentaire telle que:

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

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

– l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;

– la durée de conservation des données.“

Cette information doit avoir lieu au plus tard lors de la collecte des données. Peu importe les moyens et supports employés en vue de la collecte des données, que ce soit, par exemple, par voie de formulaire ou questionnaire standardisé ou non.

Ensuite, en application du paragraphe (2) de l'article 26, lorsque les données n'ont pas été collectées auprès de la personne concernée, que ce soit une personne liée à la personne concernée ou non, le responsable du traitement doit fournir à la personne concernée 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;

– la durée de conservation des données.“

---

1 Listes noires (listes d'adresses inaccessibles) ou listes blanches (listes d'adresses accessibles)

2 Directive, considérant 38

Dans ce cas de figure, l'information de la personne concernée a lieu „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", afin de lui permettre de faire usage de ses droits d'accès ou d'opposition.

Quelle que soit la personne qui fournit les données, les précisions suivantes s'imposent:

Il s'agit sans nul doute possible d'une obligation de résultat qui pèse sur le responsable du traitement. Celui-ci n'a pas besoin d'effectuer personnellement la collecte des données, qui peut être faite par des personnes mandatées par lui ou par ses employés[1]. En tout cas, le responsable du traitement ne peut se délier de son obligation en arguant que la collecte a été réalisée par une autre personne. Le responsable du traitement conserve cependant un recours contre la personne qui a fautivement ou intentionnellement négligé d'informer la personne concernée.

L'article 26 fait référence à la collecte des données. Ces termes impliquent la nécessité d'une démarche active du responsable du traitement. Si les données ont été fournies au responsable du traitement par la personne concernée agisant de sa propre initiative, l'article 26, paragraphe (1) ne s'applique pas. Si le responsable du traitement a reçu les données spontanément par quelqu'un d'autre que la personne concernée, l'article 26, paragraphe (2), s'applique.

L'emploi de l'adjectif „déterminées" pour caractériser les finalités devant être incluses parmi les informations à fournir à la personne concernée vise à éviter que le responsable du traitement n'indique que des finalités vagues, ce qui viderait de son sens le droit à l'information de la personne concernée.

Le responsable du traitement devra fournir toutes les informations supplémentaires nécessaires, compte tenu des circonstances particulières dans lesquelles les données sont collectées, pour assurer à l'égard de la personne concernée un traitement loyal des données, c'est-à-dire une information pleine et entière[2]. La liste de ces informations supplémentaires n'est pas exhaustive. Ainsi, par exemple, si les données n'ont pas été fournies par la personne concernée, celle-ci peut, suivant les cas, être en droit de connaître l'identité de la personne ayant fourni des données la concernant. De même l'article 30, paragraphe (1) lettres (b) et (c), oblige le responsable du traitement à informer la personne concernée de l'existence d'un droit d'opposition en cas de traitement à des fins de prospection.

La personne concernée peut en outre consulter le registre public tenu par la Commission nationale[3].

La manière dont les informations visées à l'article 26 ont été fournies à la personne concernée importe peu. Il faut cependant que l'information soit lisible et intelligible. Une information orale peut suffire[4]. En cas de contestation sur l'existence ou l'étendue de l'information fournie à la personne concernée, il appartient au responsable du traitement d'apporter la preuve qu'il a satisfait à son obligation d'information de la personne concernée.

L'information doit être fournie à la personne concernée. Le responsable du traitement ne pourra pas se satisfaire d'une information générale publiée, par exemple, dans la presse. L'information doit être ciblée.

2. Exceptions

Une première exception découle de l'article 26. Si la personne concernée a déjà été informée avant la collecte ou dès l'enregistrement des données ou au plus tard lors de la première communication de données, selon l'hypothèse retenue, le droit à information disparaît. Il se peut néanmoins que le responsable du traitement doive encore fournir certaines informations compte tenu du degré d'information préalable de la personne concernée. L'information préalable a pu être incomplète[5]. „Par ailleurs, l'exception ne joue que si la personne concernée est informée, non si elle est raisonnablement supposée être informée."[6]

Les trois autres exceptions sont répertoriées à l'article 27.

---

1 Par exemple, des personnes effectuant un sondage ou un recensement

2 Directive, articles 10 et 11, paragraphe 1

3 Article 15

4 Sauf que dans le cas d'une information orale, un problème de preuve peut se poser

5 Léonard, Poullet, op. cit., p. 389

6 Ibid., eod. loc.

En premier lieu, le droit de la personne concernée à l'information est écarté, lorsque le traitement est nécessaire pour sauvegarder:

„(a) la sûreté de l'Etat;

(b) la défense;

(c) la sécurité publique;

(d) la prévention, la recherche, la constatation et la poursuite d'infractions pénales y compris celles à la lutte contre le blanchiment[1], ou le déroulement de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 [du présent projet];

(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."

Ensuite, les impératifs de la liberté d'expression permettent également de déroger aux prescriptions de l'article 26. L'article 9 paragraphe (1), permet de déroger à l'article 26 paragraphe (1) „lorsque son application compromettrait la collecte des données auprès de la personne concernée" et à 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".

Enfin, d'après le paragraphe (3) de l'article 27, les dispositions de l'article 26 „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". Pour mesurer les „efforts disproportionnés", „peuvent être pris en considération le nombre de personnes concernées, l'ancienneté des données, ainsi que les mesures compensatrices qui peuvent être prises"[2].

B. Le droit d'accès

Le droit d'accès permet à la personne concernée de s'assurer de l'exactitude des données et des conditions de licéité et de légitimité du traitement.

1. Principe

En application de l'article 28, la personne concernée ou ses ayants droit justifiant d'un intérêt légitime peuvent demander au responsable du traitement:

„(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."

L'accès se fait sans frais. Les demandes d'accès peuvent être présentées à des intervalles raisonnables et la communication des informations se fait „sans délais excessifs".

Que la demande d'accès émane de la personne concernée ou de ses ayants droit, le demandeur doit prouver son identité. S'agissant d'un droit fondamental, le droit d'accès s'exerce sans contrainte, c'est-à-dire sans influence d'un tiers intéressé par les données traitées.

L'article 28, paragraphe (3), a trait aux données concernant un patient et recueillies par une personne exerçant une profession médicale ou un établissement hospitalier. Le droit d'accès aux données le concernant est exercé par le patient lui-même ou par l'intermédiaire d'un médecin qu'il désigne. Le

---

1 Voir article 39 de la loi du 5 avril 1993 sur le secteur financier

2 Directive, considérant 40

droit d'accès pourra encore être exercé, du vivant de la personne concernée, mais placée sous le régime de la curatelle ou sous celui de la tutelle, par l'intermédiaire d'un médecin désigné par son curateur ou tuteur.

L'article 28 indique encore que, si le patient – personne concernée est décédé, le droit d'accès aux données relatives au de cujus est exercé par l'intermédiaire d'un médecin désigné par le conjoint non séparé de corps et ses enfants ou par toute personne qui au moment du décès a vécu avec lui dans le ménage ou encore, s'il s'agit d'un mineur, par ses père et mère. Il s'agit de la reprise de l'article 36, alinéa 5, de la loi du 28 août 1998 sur les établissements hospitaliers.

Que se passe-t-il si la personne concernée, qui n'est pas placée sous un régime de protection, est dans l'incapacité physique[1] soit d'exercer elle-même son droit d'accès, soit de désigner un médecin à cette fin? Dans pareille hypothèse, le droit d'accès devrait s'exercer par les mêmes personnes investies du droit d'exercer à la place de la personne concernée le droit d'accès en cas de décès de celle-ci.

Si la personne qui a exercé 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", elle peut en informer la Commission nationale qui procède aux vérifications nécessaires[2].

Le paragraphe (5) de l'article 28 impose au responsable du traitement de rectifier, effacer ou verrouiller les données qui n'ont pas été traitées en conformité des dispositions du projet de loi, notamment en raison du caractère incomplet ou inexact des données. Faute de ce faire, la Commission nationale peut ordonner l'interdiction temporaire ou définitive du traitement ou la destruction des données. Toute rectification, effacement ou verrouillage doit être notifié sans délai par le responsable du traitement aux destinataires auxquels les données ont été communiquées.

Cette notification exigée par l'article 28, paragraphe (7) et figurant déjà à l'article 23 de la loi du 31 mars 1979, ne doit pas avoir lieu si elle s'avère impossible. „Impossible" ne signifie pas une notification trop chère ou exigeant des efforts disproportionnés. L'impossibilité vise une impossibilité technique ou matérielle. Ainsi le projet de loi est-il plus restrictif que la directive qui, dans son article 12, lettre c., dispense de la notification non seulement lorsque cela s'avère impossible, mais aussi lorsqu'une telle communication suppose un effort disproportionné. Cette dernière justification pour se dispenser de communiquer aux tiers toute rectification, effacement ou verrouillage n'a pas été reprise dans le projet de loi. La protection des droits de la personne concernée s'en trouve renforcée.

2. Exceptions

Les exceptions au droit d'accès sont du même ordre que celles visant le droit à l'information.

Il y a d'une part, la liberté d'expression visée tant à l'article 28, paragraphe (4), qu'à l'article 29, paragraphe (1) lettre (g).

Ensuite, l'article 29, paragraphe (1) énumère les mêmes exceptions que celles figurant à l'endroit de l'article 27, paragraphe (1), en y ajoutant cependant la mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés à l'article 29, paragraphe (1) aux lettres (c) [sécurité publique], (d) [infractions pénales] et (e) [intérêt économique ou financier important].

Le droit d'accès peut aussi être limité, en vertu de l'article 29, paragraphe (2), à condition:

– qu'il s'agisse de données traitées exclusivement à des fins de recherche scientifique ou de données stockées pour une durée n'excédant celle nécessaire à la seule finalité d'établissement de statistiques;
– qu'il n'existe manifestement aucun risque d'atteinte à la vie privée d'une personne concernée;
– que ces données ne puissent être utilisées aux fins de prendre une mesure ou une décision se rapportant à des personnes précises.

En toute hypothèse, le responsable du traitement doit indiquer au demandeur le motif pour lequel il limite ou diffère l'exercice du droit d'accès. Lorsque le droit d'accès est différé, il doit encore indiquer la date à partir de laquelle le droit d'accès peut à nouveau être exercé[3].

---

1 Parce que, par exemple, elle se trouve dans un état comateux

2 Article 28, paragraphe (6)

3 Article 29, paragraphe (3)

Le motif de refus de donner accès est notifié par le responsable du traitement à la Commission nationale[1] pour que celle-ci soit à même de remplir sa mission de surveillance et de prendre les mesures qui s'imposent. En effet, au vœu de l'article 29, paragraphe (4), en cas de limitation de l'exercice du droit d'accès, le droit d'accès est exercé indirectement par la Commission nationale. Celle-ci dispose d'un pouvoir d'investigation en la matière et fait opérer la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme au présent projet de loi. L'article 29, paragraphe (4), précise que „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".

C. Le droit d'opposition

Le droit d'opposition est un droit qui n'existait pas sous l'empire de la loi du 31 mars 1979.

Le droit d'opposition peut être invoqué dans les deux cas de figure mentionnés à l'article 30, paragraphe (1).

1. La personne concernée a le „droit 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 oeuvre par le responsable du traitement ne peut pas porter sur ces données" (lettre (a)).

   La personne concernée peut s'opposer à ce que des données soient traitées. Elle ne peut s'opposer au traitement en soi, sauf si le traitement est interdit en vertu d'une disposition législative ou réglementaire.

2. La seconde possibilité pour la personne concernée d'exercer son droit d'opposition concerne les traitements réalisés à des fins de prospection[2].

   La personne concernée peut „s'opposer, sur demande et gratuitement, au traitement la concernant envisagé par le responsable du traitement 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" (lettre (b)). Dans cette hypothèse, le droit d'opposition porte sur le traitement et non pas, comme indiqué à la lettre (a), sur la donnée.

   Le Conseil d'Etat avait suggéré de supprimer cette disposition, alors qu'elle ferait „dans une large mesure" double emploi avec l'article 48 de la loi du 14 août 2002 relative au commerce électronique.

   La commission a cependant estimé que la suppression de la lettre (b) réduirait la protection de la personne concernée. Dans le cadre de l'article 14 de la directive, la notion de prospection peut recouvrir des significations plus variées que celle visée à l'article 48 de la loi du 14 août 2000. L'article 30 couvre également la prospection à but non commercial.

   De plus, conformément à l'article 1er, paragraphe (5) lettre b), et au considérant 14 de la directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information, le commerce électronique est entièrement soumis aux dispositions législatives en matière de protection des données comprises dans les directives 95/46/CE et 97/66/CE.

   Enfin, l'article 7, paragraphe (2), de la directive 2000/31/CE ne fait que définir les modalités d'une des deux formes possibles (à savoir l'opt out) du droit d'opposition.

   La définition des champs respectifs de ces deux formes (opt in/opt out) est faite par renvoi aux directives 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications et 97/7/CE concernant la vente à distance des biens et des services autres que les services financiers.

   Dès lors, la transposition du principe du droit d'opposition visé à l'article 14 de la directive et à l'article 30 du projet de loi ne saurait se satisfaire de l'article 48 de la loi sur le commerce électronique vu son champ d'application et son contenu.

3. La personne concernée a le droit 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 prospec-

---

1 ibid.

2 Encore appelée „marketing direct"

tion et de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation" (lettre (c)). Le fait de se „voir offrir le droit de s'opposer" signifie que la personne concernée doit être informée du droit de faire opposition. Cette disposition ne se substitue pas à l'article 26: le responsable du traitement doit indiquer, entre autres, les finalités déterminées poursuivies par le traitement et les tiers qui recevront communication des données collectées.

D. Les décisions individuelles automatisées

L'article 31 permet à une personne d'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."

La première hypothèse suppose l'existence d'un contrat (par exemple, credit-scoring).

La seconde hypothèse concerne surtout le secteur public.

Le principe est d'éviter que des décisions automatisées produisent des effets juridiques à l'égard de la personne concernée. Les travaux préparatoires de la loi belge du 11 décembre 1998 commentent cette disposition comme suit: „cette disposition doit éviter que, sans aucune intervention humaine, des décisions sont prises directement sur la base d'un résultat d'un traitement automatisé." De même, „on respecte donc la disposition lorsque entre l'obtention du résultat du traitement par ordinateur et la prise de décision il y ait au moins une intervention humaine minimale"[1].

*

IV. LES FORMALITES DE MISE EN OEUVRE DU TRAITEMENT

Le mécanisme mis en place par la loi du 31 mars 1979 pêchait par sa lourdeur. Toute banque de données était soumise à autorisation préalable. Le projet de loi sous rubrique introduit une nouvelle philosophie en ce que les banques de données ne sont plus en tant que telles soumises à une quelconque procédure administrative. Ce sont les traitements qui sont visés. En outre, remplaçant la procédure d'autorisation, le projet de loi institue le principe d'une simple notification (A.) tout en maintenant dans des situations particulières notamment lorsque des données susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées, l'obligation d'une autorisation préalable (B.).

Les notifications et autorisations figureront sur un registre public (C.).

A. Le principe: la notification préalable du traitement

Le principe est posé à l'article 12, paragraphe (1), qui dispose que les traitements font l'objet d'une notification préalable par le responsable du traitement auprès de la Commission nationale. Cette notification préalable au commencement du traitement permet à la Commission nationale d'exercer son contrôle a posteriori, lequel doit être considéré comme „une mesure suffisante"[2] pour la sauvegarde des droits et libertés des personnes concernées.

En application de l'article 13, paragraphe (3), la notification se fait auprès de la Commission nationale moyennant support papier ou informatique suivant un schéma à établir par elle[3]. La Commission nationale accuse réception de la notification. Un règlement grand-ducal, pris sur base des articles 13, paragraphe (5) et 37, paragraphe (4), peut fixer le principe et le montant d'une redevance à payer pour

1 Exposé des motifs, p. 17, cité in Léonard, Poullet, op. cit., p. 391

2 Directive, considérant 52

3 Voir article 43, paragraphe (1)

toute notification ou modification de notification. Cette redevance constitue la contrepartie des frais de personnel et de fonctionnement de la Commission nationale.

Le risque de voir la Commission nationale submergée par une multitude de notifications a amené le législateur à prévoir des aménagements ou dérogations à l'obligation de notification.

D'abord, 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[1]. Un traitement poursuivant différentes finalités, à condition que celles-ci soient liées entre elles, ou plusieurs traitements poursuivant la même finalité, peuvent faire l'objet d'une seule et même notification.

Ensuite, la Commission nationale établit et publie des directives[2] en vue d'une notification simplifiée pour les traitements des données dont la mise en œuvre n'est pas susceptible de porter atteinte aux libertés et droits fondamentaux, et notamment à la vie privée, des personnes concernées.

L'article 12, paragraphe (2) précise le contenu de ces directives de notification simplifiée et indique que „les traitements qui correspondent à ces directives font l'objet d'une notification simplifiée de conformité envoyée à la Commission nationale le cas échéant par voie électronique".

Enfin, conformément aux paragraphes (1) et (3) de l'article 12, sont exemptés de l'obligation de notification:

a. le traitement effectué en application de l'article 8, y compris le traitement mis en œuvre conformément aux règles de procédures judiciaires en matière civile et nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice;
b. le traitement qui doit être préalablement autorisé par la Commission nationale (article 14);
c. le traitement qui doit être autorisé par voie réglementaire (article 17);
d. le responsable du traitement qui désigne un chargé de la protection des données[3]. Ce chargé de la protection des données établit un registre des traitements effectués par le responsable du traitement et continue ce registre à la Commission nationale;
e. „le traitement ayant pour seul objet 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"[4], comme par exemple le registre du commerce et des sociétés.

Le contenu de la notification est détaillé à l'article 13. Rappelons que, d'après l'article 9, paragraphe (2), en cas de notification d'un traitement réalisé à des fins de journalisme ou d'expression artistique ou littéraire, seuls les nom et adresse du responsable du traitement ou de son représentant sont exigés.

Il va de soi que toute modification de l'une des informations devant figurer dans la notification doit être à son tour notifiée à la Commission nationale.

B. L'exception: l'autorisation préalable du traitement

Cette autorisation découle soit d'une décision de la part de la Commission nationale (1.), soit d'un règlement grand-ducal (2.).

1. L'autorisation préalable par la Commission nationale

Eu égard à l'importance de certaines données ou à leur caractère sensible, une notification préalable ne suffit pas. Constatant que „certains traitements sont susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées, du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, ou du fait de l'usage particulier d'une technologie nouvelle"[5], la directive permet en son article 20 aux Etats membres de préciser „les traitements susceptibles de présenter des risques particuliers

---

1 Article 12, paragraphe (1) lettre (b)

2 Le terme de „directive" a été préféré à celui de „norme" „afin de ne pas laisser entrevoir que la Commission nationale disposerait en la matière d'un pouvoir réglementaire au sens propre du terme" (Conseil d'Etat, avis complémentaire, sub Article 12)

3 Voir V. B. 2. ci-après

4 Article 12, paragraphe (3) lettre (b)

5 Directive, considérant 53

au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en oeuvre".

Présentent ces „risques particuliers" et sont donc soumis à l'autorisation préalable de la Commission nationale[1]:

a. les traitements de données sensibles pour lesquels la personne concernée doit donner son consentement (article 6, paragraphe (2) lettre (a))[2];

b. les traitements de données sensibles nécessaires pour faire respecter les obligations et droits spécifiques du responsable du traitement, notamment en matière de droit du travail dans la mesure où ce traitement est autorisé par la loi (article 6, paragraphe (2) lettre (b));

c. les traitements de données sensibles rendues manifestement publiques par la personne concernée (article 6, paragraphe (2) lettre (e));

d. les traitements de données sensibles nécessaires pour un motif d'intérêt public, notamment à des fins historiques, statistiques ou scientifiques (article 6, paragraphe (2) lettre (g));

e. les traitements des données génétiques visés à l'article 6, paragraphe (4) lettre (b);

f. les traitements de données par les services de la santé conformément à l'article 7, paragraphe (1);

g. les traitements aux fins de surveillance (article 10);

h. les traitements aux fins de surveillance sur le lieu de travail (article 11);

i. les traitements de données collectées pour une finalité déterminée, mais destinées à être traitées ultérieurement pour des fins historiques, statistiques ou scientifiques (article 4, paragraphe (2))[3];

j. l'interconnexion de données à caractère personnel de l'article 16. Sont visées les interconnexions qui ne sont pas prévues par un texte légal ou réglementaire.

   Une interconnexion se définit comme „toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d'autres responsables du traitement"[4].

   Les responsables des traitements en cause doivent présenter une demande conjointe à la Commission nationale aux fins de l'interconnexion. L'interconnexion peut concerner des traitements autorisés par et/ou notifiés à la Commission nationale. Il faudra de toute façon qu'il y ait déjà eu autorisation ou notification. Cependant rien n'interdit une demande d'interconnexion qui soit concomitante avec une ou plusieurs demandes d'autorisation ou une ou plusieurs notifications.

   La finalité poursuivie par cette interconnexion est indiquée au paragraphe (2) de l'article 16: „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." La discrimination visée s'entend à la fois d'une discrimination directe que d'une discrimination indirecte.

   Les finalités des traitements dont l'interconnexion est demandée doivent être identiques ou liées. La Commission nationale devra également veiller au respect du secret professionnel auquel sont astreintes certaines professions.

   La commission estime que l'élaboration de textes législatifs ou réglementaires autorisant une interconnexion de données devra s'inspirer de la ratio des dispositions de l'article 16;

k. les traitements concernant le crédit et la solvabilité des personnes concernées;

---

1 Dans son avis complémentaire du 2 juillet 2002, le Conseil d'Etat a donné à considérer si l'on ne devait pas soumettre à autorisation préalable les traitements visés à l'article 6, paragraphe (2) lettre (d), à savoir les traitements mis en oeuvre du consentement de la personne concernée par des organismes à finalité politique, philosophique, religieuse ou syndicale. La commission a décidé de ne pas reprendre la proposition du Conseil d'Etat, dans la mesure où cette extension risquerait d'entrer en conflit avec d'autres libertés fondamentales garanties par la Constitution et la Convention européenne des droits de l'homme

2 Comme l'autorisation doit être préalable au début du traitement, la personne concernée n'a pas pu donner son consentement. Il s'agit donc des traitements auxquels la personne doit consentir, sans que le consentement ait encore pu être obtenu

3 Il est renvoyé au point II. A. 1. a. ci-dessus

4 Article 2, lettre (j)

l. l'utilisation de données à des fins autres que celles pour lesquelles elles ont été collectées. L'article 14, paragraphe (1) lettre (e), précise, conformément au principe de finalité, qu'un „tel traitement ne peut être effectué que moyennant le consentement préalable de la personne concernée".

A l'instar des notifications uniques de l'article 12, l'article 14, paragraphe (3), permet à la Commission nationale d'autoriser par une décision unique plusieurs traitements qui ont une même finalité, qui portent sur des catégories de données identiques et qui ont les mêmes destinataires ou catégories de destinataires. Dans la mesure où l'autorisation est préalable au commencement du traitement, le responsable du traitement adresse à la Commission nationale un engagement formel de conformité du traitement à la description figurant dans l'autorisation.

Le paragraphe (2) de l'article 14 indique le contenu d'une demande en autorisation. Le parallèle avec l'article 13, paragraphe (1), relatif au contenu d'une notification est évident. Cependant, les dispositions des lettres (e) et (f) ainsi que de la lettre (i) de l'article 14, paragraphe (2) sont plus restrictives qu'à l'article 13, paragraphe (1) lettres (d) et (g). En effet, au regard des risques particuliers des traitements soumis à autorisation au regard des droits et libertés fondamentaux des personnes concernées, il a paru nécessaire de demander des informations plus détaillées sur les données concernées et traitements envisagés ainsi que sur les mesures de sécurité que dans le cadre d'une notification. Les termes „description détaillée" qui figurent à l'article 14, paragraphe (2) lettres (e) et (i), démontrent l'exigence d'une précision non requise à l'endroit de l'article 13.

2. L'autorisation par règlement grand-ducal

Deux catégories de traitements doivent être autorisées par règlement grand-ducal. Elles sont limitativement énumérées à l'article 17, paragraphe (1). Il s'agit:

a. des „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" du projet de loi. Cette disposition s'inspire de l'article 12-1 de la loi modifiée du 31 mars 1979.

   Sur proposition du Conseil d'Etat contenue dans son avis complémentaire, la commission a supprimé de la disposition précitée la „poursuite des infractions pénales". En effet, comme le note à juste titre le Conseil d'Etat, d'opérer une séparation nette entre les traitements visés à l'article 17 et ceux relevant de l'article 8 dans le champ d'application duquel tombent précisément les actes de poursuite.

b. des „traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique" et

c. des „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)".

Ces traitements autorisés par règlement grand-ducal peuvent être effectués tant en application d'une disposition de droit interne qu'en application d'une convention internationale.

En raison de la sensibilité des traitements précités, prolongeant le régime de l'article 12-1, paragraphe (4), de la loi du 31 mars 1979, le contrôle et la surveillance de ces traitements ne sont pas exercés par la Commission nationale, mais par une autorité de contrôle ad hoc 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[1].

Un règlement grand-ducal déterminera l'organisation et le fonctionnement de cette autorité de contrôle.

L'autorité de contrôle est informée immédiatement de la mise en œuvre d'un traitement de données autorisé par règlement grand-ducal. Elle veille à ce que ces traitements soient effectués conformément aux dispositions légales qui les régissent.

---

1 Ce terme est défini à l'article 2, lettre (k)

L'article 17, paragraphe (2) décrit les pouvoirs de cette autorité comme suit:

„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 ci-dessus.

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 intéressée que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exécution."

C. Le registre public

La Commission nationale tient un registre public sur lequel figurent, conformément à l'article 15, paragraphe (2), les traitements notifiés en vertu de l'article 12, paragraphe (1), les traitements autorisés en application de l'article 14, paragraphe (1) ainsi que les traitements faisant l'objet d'une surveillance par le chargé de la protection des données.

C'est d'ailleurs une des raisons qui explique que le registre tenu par le chargé de la protection des données devra être continué à la Commission nationale[1].

Ne figurent pas sur ce registre les „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"[2], comme par exemple le registre du commerce et des sociétés.

Au vœu de l'article 15, paragraphe (3), le registre public renseigne les informations devant être communiquées à la Commission nationale dans le cadre de la notification ou de la demande d'autorisation. Partant ces mêmes informations doivent également figurer sur le registre tenu par le chargé de la protection des données.

S'agissant d'un registre public, toute personne peut gratuitement prendre connaissance des informations y figurant. Pour des raisons évidentes, les informations portant sur les mesures de sécurité exigées par les articles 13, paragraphe (1) lettre (g) et 14, paragraphe (2) lettre (i), ne sont pas consultables.

Il est précisé que ce registre est en ligne, ce qui permet une consultation plus aisée.

En application de l'article 15, paragraphe (5), 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,

(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 de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi,

(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

---

1 Article 12, paragraphe (3) lettre (a)

2 Article 15, paragraphe (7)

(i) le secret professionnel et le secret d'affaires de la personne concernée et du responsable du traitement".

On retrouve ici les limitations similaires au droit d'accès de la personne concernée visées à l'article 29.

*

V. LE CONTROLE DU TRAITEMENT

Le contrôle du respect de la conformité des traitements de données aux dispositions du projet de loi est double. D'un côté, il est effectué par un établissement public indépendant, la Commission nationale (A.). De l'autre, un tel contrôle peut se faire en interne, par l'intermédiaire du chargé de la protection des données et en respectant les mesures de sécurité requises (B.).

A. Le contrôle externe: la Commission nationale pour la protection des données

La commission consultative visée à l'article 30 de la loi du 31 mars 1979 a été rapidement débordée par la tâche qui lui a été confiée. Afin d'assurer un contrôle efficace des dispositions du projet de loi, celui-ci institue une autorité indépendante organisée sous forme d'un établissement public, la Commission nationale. Cette Commission nationale „est un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel"[1].

Elle est „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, 3]. Le projet de loi donne à cette autorité tous les moyens nécessaires à une bonne exécution de ses missions afin d'éviter que ne se reproduisent les mêmes problèmes que ceux survenus lors de l'exécution de la loi du 31 mars 1979.

L'échec de la Commission nationale dans l'accomplissement de sa mission signifierait vraisemblablement en même temps l'échec de l'application du projet de loi.

1. Statut de la Commission nationale[4]

La Commission nationale est un établissement public indépendant. Elle est dotée de la personnalité juridique, jouit de l'autonomie financière et administrative et est placée sous l'autorité du membre du gouvernement ayant la protection des données dans ses attributions.

Son siège est fixé à Luxembourg-ville, mais peut être transféré à tout moment dans un autre endroit du Luxembourg par règlement grand-ducal. Le transfert du siège de la Commission nationale est un acte réglementaire, car il affecte l'organisation de la Commission nationale.

La Commission nationale est composée de trois membres effectifs, à savoir un président et deux membres effectifs, et de trois membres suppléants. Ces membres sont nommés par le Grand-Duc sur proposition du Gouvernement en conseil pour un terme de 6 ans, renouvelable une fois. 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 sont révoqués par le Grand-Duc sur proposition du Gouvernement en conseil. L'article 35, paragraphe (7), précise qu'avant toute révocation, la Commission nationale est entendue et pas seulement demandée en son avis. Dans le respect du fonctionnement des institutions, la Commission est obligée de donner son avis et ne saurait bloquer l'application de l'article 35 en retenant de manière déraisonnable son avis. Certes il ne s'agit que d'une consultation, mais le but est d'éviter le risque d'une influence du gouvernement sur la Commission nationale, ce qui remettrait en cause son indépendance.

---

1 Directive, considérant 62

2 Article 32, paragraphe (1)

3 L'article 17, paragraphe (2) institue un organisme spécifique pour la surveillance des traitements opérés dans le cadre d'une autorisation par voie réglementaire: voir IV. B. 2.

4 Articles 34 à 37

Le successeur d'un membre qui cesse l'exercice de ses fonctions reste en fonction pour la durée du mandat restant à courir.

Tant parmi les membres effectifs que parmi les membres suppléants figurent au moins un juriste et un informaticien justifiant d'une formation universitaire adéquate.

Le président est désigné par le Grand-Duc et prête serment entre les mains du Grand-Duc ou de son représentant. Les autres membres de la Commission nationale prêtent serment entre les mains du président.

Les incompatibilités de fonctions sont mentionnées à l'article 34, paragraphe (3), à savoir „membre du Gouvernement, de la Chambre des Députés, du Conseil d'Etat ou du Parlement Européen" et l'exercice d'activité professionnelle ou la détention directe ou indirecte d'intérêts dans une entreprise ou tout autre organisme opérant dans le champ des traitements de données.

Le statut des membres effectifs de la Commission nationale est réglé à l'article 24 du projet de loi. Ce statut est calqué sur celui prévu à l'article 9 du projet de loi sur la promotion des droits de l'enfant et la protection sociale de l'enfance[1].

Les membres suppléants touchent une indemnité dont le montant est fixé par règlement grand-ducal[2].

La commission nationale est assistée d'agents, d'employés et d'ouvriers[3]. Elle peut recourir à des experts externes engagés sur base d'un contrat de droit privé[4].

La Commission est un organe collégial. Elle se dote d'un règlement d'ordre intérieur.

Les réunions de la Commission nationale sont convoquées par le président. La Commission nationale doit se réunir à la demande de deux membres effectifs. La convocation est adressée aux seuls membres effectifs et contient l'ordre du jour de la réunion. Si les membres effectifs sont empêchés d'assister à une réunion, ils en avertissent les membres suppléants.

Le quorum de présence est de trois membres. Les décisions sont prises à la majorité des voix, étant entendu qu'il ne saurait y avoir d'abstention. Seuls des votes pour ou contre la proposition figurant à l'ordre du jour sont admissibles.

Aucun membre ne peut assister à une réunion de celle-ci, ni délibérer ni décider dans une affaire où il a un intérêt direct ou indirect. La violation de cette règle fondamentale prescrite à l'article 35, paragraphe (5), entraîne la nullité absolue de la décision prise. Le membre ayant un conflit d'intérêts devra se faire remplacer par un membre suppléant.

La Commission nationale publie chaque année un rapport à l'attention des membres du Gouvernement en conseil. Ce rapport renseigne, entre autres, l'exécution de ses missions et 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[5].

S'agissant de l'avis de la CCDH, la commission s'exprime en principe en faveur de l'implication d'une commission consultative des droits de l'homme, dont l'instauration a été demandée par certains représentants des „forces vives de la nation" afin d'assurer une certaine surveillance de la Commission nationale et un regard critique sur les avis de cette autorité. La CCDH est un organe consultatif du Gouvernement en matière de droits de l'homme qui trouvera ainsi une base légale, alors que son fonctionnement interne actuellement régi par l'arrêté ministériel du 26 mai 2000.

Les dispositions financières, comprenant les obligations de la Commission nationale d'arrêter annuellement son compte d'exploitation et d'établir un budget, sont répertoriées à l'article 37.

---

1 Doc. parl. 4137

2 Article 34, paragraphe (2) dernier alinéa

3 Article 35, paragraphes (1) à (3)

4 Article 36, paragraphe (4)

5 Articles 15, paragraphe (6) et 32, paragraphe (2)

2. Missions et pouvoirs de la Commission nationale

D'après l'article 34, paragraphe (1) alinéa 3, la Commission nationale exerce en toute indépendance les missions qui lui sont confiées. Ses membres effectifs et suppléants ne reçoivent aucune instruction de quelque autorité que ce soit[1].

Les missions et pouvoirs de la Commission nationale sont énumérés à l'article 32, paragraphe (3).

La Commission nationale assure l'application des dispositions du projet de loi et de ses règlements d'exécution en particulier celles relatives à la confidentialité et à la sécurité des traitements.

Elle reçoit les notifications préalables et autorise les traitements. Elle assure la publicité des traitements en tenant un registre afférent dans les conditions de l'article 15.

La Commission nationale est 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 dans son rapport annuel.

La Commission nationale a le droit de présenter au Gouvernement toutes suggestions susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données. Elle conseille le Gouvernement sur les conséquences de l'évolution des technologies de traitement de l'information au regard du respect des libertés et droits fondamentaux des personnes. Pour ce faire, elle peut faire procéder à des études, des enquêtes ou expertises.

Elle reçoit et, le cas échéant après discussion avec les auteurs, approuve les codes de conduite relatifs à un traitement ou un ensemble de traitements lui soumis par des associations professionnelles représentatives de responsables du traitement.

Elle „favorise 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"[2].

La saisine de la Commission nationale s'opère par toute personne, agissant par elle-même, par l'entremise de son avocat ou par toute autre personne physique ou morale dûment mandatée afin de faire respecter ses droits et libertés fondamentaux à l'égard d'un traitement. La personne concernée est informée des suites réservées à sa requête.

La personne concernée peut demander à la Commission nationale de vérifier la licéité d'un traitement en cas de refus ou de limitation de l'exercice du droit d'accès de la personne concernée conformément à l'article 29, paragraphe (4).

Si la Commission nationale est saisie par l'une des personnes ou organes visés à l'article 11, paragraphe (2), sur une violation de cet article[3], elle statue dans le mois de la saisine. Dans les autres cas, la législation sur la procédure administrative non contentieuse s'applique, la Commission nationale étant à considérer comme autorité administrative. Le silence de la Commission nationale pendant une durée de trois mois vaut donc rejet de la demande présentée par la personne concernée ou par les autres personnes mentionnées à l'article 32, paragraphe (4).

La Commission nationale dispose d'un pouvoir d'investigation en vertu duquel elle a accès aux données faisant l'objet du traitement en question et recueille toutes les informations nécessaires à l'accomplissement de sa mission de contrôle. Elle a un accès direct aux locaux autres que les locaux d'habitation où a lieu le traitement ainsi qu'aux données faisant l'objet du traitement et procède aux vérifications nécessaires.

La Commission nationale a le droit d'ester en justice pour faire respecter les dispositions du projet de loi et des règlements grand-ducaux pris dans le cadre de ce projet de loi. Dans les conditions fixées à l'article 39, elle peut saisir le président du tribunal d'arrondissement où le traitement a eu lieu d'une action en cessation. Elle dénonce aux autorités judiciaires les infractions dont elle a connaissance qui pourront déclencher une action publique si l'infraction ainsi dénoncée est sanctionnée pénalement et/ou qui pourront intenter eux-mêmes l'action en cessation prévue par l'article 39.

---

1 Article 35, paragraphe (8)

2 Article 32, paragraphe (3) lettre (i)

3 Traitements aux fins de surveillance sur le lieu du travail

En vertu de l'article 33, „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".

Les sanctions prises par la Commission nationale peuvent faire l'objet d'un recours en réformation suivant l'article 3 de la loi du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif.

Sur le plan international, la Commission nationale coopère avec 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. 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.

B. Le contrôle interne

Ce contrôle interne comporte deux volets. Le premier consiste pour le responsable du traitement de prendre toutes les mesures de sécurité nécessaires pour assurer la sécurité des traitements (1.). Le second est une innovation du projet de loi qui prévoit l'institution d'un chargé de la protection des données (2.).

1. Subordination et sécurité des traitements

L'article 21 dispose que „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".

Conformément à l'article 24, paragraphe (1), l'article 458 du Code pénal s'applique aux membres de la Commission nationale et à toute personne qui accomplit une mission pour son compte ainsi qu'au chargé de la protection des données. Cette obligation perdure même après la fin de leur fonction.

Même si le projet de loi ne le prévoit pas expressis verbis, il en va de même pour les responsables du traitement et les personnes visées à l'article 21, alors qu'il s'agit de „personnes dépositaires, par état ou par profession, des secrets qu'on leur confie". Il en va de même pour toute personne travaillant pour la Commission nationale et ayant accès à des informations confidentielles.

Le projet de loi précise, en son article 24, paragraphes (2) et (3) que le chargé de la protection des données agissant dans le cadre de l'accomplissement de ses missions et le prestataire de service de certification ne peuvent opposer à la Commission nationale le secret professionnel auquel ils sont soumis[1]. De même en vertu du paragraphe (4) de cet article, s'agissant du traitement de données sensibles par les services de la santé prévu à l'article 7, „le responsable du traitement agissant dans le cadre de l'accomplissement de ses missions visées à l'article 7, paragraphe (1), 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)". La référence à l'article 32, paragraphe (6) a été supprimée sur proposition du Conseil d'Etat et pour les motifs contenus dans son avis complémentaire.

Conformément à l'avis du Conseil d'Etat, il y a lieu d'encadrer l'accès aux données relatives à la santé. Toutefois cet encadrement ne peut consister en une limitation des types de renseignements accessibles. La protection de la vie privée de la personne concernée se limite à la seule hypothèse dans laquelle la Commission nationale agirait de son propre chef. Dès lors qu'elle est saisie sur requête de la personne concernée, rien ne s'oppose à ce que la Commission nationale ait accès aux données du demandeur.

---

1 Le secret professionnel du prestataire de service de certification est régi par l'article 19 de la loi du 14 août 2000 relative au commerce électronique

Les règles concernant la sécurité du traitement sont énumérées aux articles 22 et 23.

Eu égard à la nature des données, la sécurité du traitement revête un caractère particulièrement important.

> „Le responsable du traitement doit mettre en œuvre toutes les mesures techniques et d'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[1].“

Ces mesures de sécurité doivent être communiquées à la Commission nationale dans le cadre de la notification ou de l'autorisation. En vertu de l'article 15, paragraphe (4), les indications fournies par le responsable du traitement à cette occasion ne seront pas accessibles dans le cadre de la consultation de ce registre.

Les mesures de sécurité font l'objet d'un rapport annuel à soumettre par le responsable du traitement à la Commission nationale.

Les mesures de sécurité doivent également être respectées par toute personne qui agit sous l'autorité du responsable du traitement. A cet effet, le sous-traitant choisi par le responsable du traitement doit apporter „des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer“[2]. Il appartient au responsable du traitement et au sous-traitant de veiller au respect de ces mesures.

Le sous-traitant doit avoir conclu par écrit un contrat ou un autre acte juridique dans lequel il est clairement stipulé, d'une part, que, conformément à l'article 21, il n'agit que sur la seule instruction du responsable du traitement, et d'autre part, que les obligations de sécurité des traitements lui incombent également. Il s'agit là du contenu minimal de cet écrit qui peut détailler les moyens de sécurité à mettre obligatoirement en œuvre par le sous-traitant et préciser les obligations respectives en la matière.

Les mesures de sécurité doivent englober un certain nombre de contrôles spécifiés à l'article 23. Cet article indique que, conformément au principe de proportionnalité, la mise en œuvre de ces contrôles doit être 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 place et à l'application de ces mesures. Lorsqu'il doit mettre en pratique ce critère de proportionnalité, le responsable du traitement s'attachera d'abord à tenir compte du risque d'atteinte à la vie privée. Le fait que ce critère prime celui lié à l'état de l'art et celui des coûts de mise en œuvre résulte de l'article 1er du projet de loi et, en général, de la ratio legis de l'ensemble du projet de loi.

Les contrôles visés à l'article 23 reprennent ceux énumérés à l'article 118 de la Convention de Schengen. Il s'agit du:

a. contrôle à l'entrée des installations où sont traitées des données;
b. contrôle des supports de données pour éviter un accès par une personne non autorisée;
c. contrôle de la mémoire afin d'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;
d. contrôle de l'utilisation;
e. contrôle de l'accès d'un système de traitement automatisé de données;
f. contrôle de la transmission;
g. contrôle de l'introduction pour pouvoir vérifier et constater 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;
h. contrôle du transport de données;
i. contrôle de la disponibilité par l'établissement de copies de sécurité.

L'ensemble de ces mesures doit conférer un „niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger“[3].

---

1 Article 22, paragraphe (1)

2 Article 22, paragraphe (2)

3 Directive, article 17, paragraphe 2

2. Le chargé de la protection des données

Le chargé de la protection des données, dont l'existence s'inspire de l'expérience allemande des „Datenschutzbeauftragten", peut être nommé par le responsable du traitement. Il n'y a pas d'obligation pour le responsable du traitement de nommer un tel chargé de la protection des données. Le responsable du traitement aura peut-être intérêt à le faire, alors que ce chargé peut se substituer dans certains cas à la Commission nationale et qu'il peut, mieux que la Commission nationale, car plus près du responsable du traitement, conseiller et guider celui-ci dans l'application des dispositions du présent projet de loi. La subsidiarité et parfois la complémentarité du chargé par rapport à la Commission nationale devront permettre de limiter „l'ampleur bureaucratique du contrôle"[1, 2].

Nous examinerons successivement le statut du chargé de la protection des données, puis ses missions et pouvoirs, étant entendu que l'article 40 permet en son paragraphe (10) à un règlement grand-ducal de fixer 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.

Une fois désigné et pour le temps de ses fonctions, les traitements de données se font sous sa responsabilité. L'ampleur de sa tâche est à la hauteur de l'activité du responsable du traitement.

Le responsable du traitement désigne le chargé de la protection des données et communique l'identité de celui-ci à la Commission nationale. Il n'y a pas de durée maximale pour exercer les fonctions de chargé de la protection des données.

L'article 40, paragraphe (3), prend le soin de préciser que dans l'exercice de ses missions le chargé de la protection des données est indépendant vis-à-vis du responsable du traitement. Il en découle qu'il ne saurait y avoir ni lien de subordination ni contrat de travail entre le responsable du traitement et le chargé de la protection des données. Ce dernier est un prestataire de services indépendant.

En raison de son indépendance, le chargé de la protection des données ne peut être révoqué par le responsable du traitement pour des raisons liées à l'exercice de ses missions, hormis le cas de la violation de ses obligations légales ou conventionnelles[3].

Qui peut être nommé chargé de la protection des données? Pour répondre à cette question, il convient de se référer à l'article 40, paragraphes (5) à (10).

Le chargé de la protection des données peut être soit une personne physique soit une personne morale. Il doit être agréé par la Commission nationale. Pour ce faire, le candidat à cette fonction doit justifier avoir accompli une formation universitaire en droit, économie, gestion d'entreprise, sciences de la nature, ou informatique. Il doit en outre disposer d'assises financières de vingt mille euros.

Cependant les membres de certaines professions réglementées peuvent être agréés par la Commission nationale sans autre condition. Il s'agit des avocats à la Cour[4], des réviseurs d'entreprises, des experts-comptables et des médecins. Cette liste peut être complétée par règlement grand-ducal.

En tout cas, la Commission nationale vérifie les qualités de tout chargé de la protection des données. Elle peut s'opposer à tout moment à sa désignation ou à son maintien, 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 à caractère personnel et que cette relation fait naître un conflit d'intérêts limitant son indépendance"[5]. Par exemple, un avocat qui défend le responsable du traitement dans le cadre d'un litige et le réviseur d'entreprises qui contrôle les comptes annuels de ce responsable ont un conflit d'intérêts manifeste. Il faudra être circonspect avec ceux qui étaient en relation avec le responsable du traitement, mais ne le sont plus au moment où ils sont désignés.

---

1 Doc. parl. 4735, p. 50

2 A noter qu'un chargé de la protection des données devrait également être institué au sein des institutions communautaires: voir proposition de décision du Parlement européen, du Conseil et de la Commission relative au statut et aux conditions générales d'exercice des fonctions de contrôleur européen de la protection des données (COM(2001) 411 – C5-0384/2001 – 2001/2150(ACI))

3 Article 40, paragraphe (3), lettre (b)

4 Seuls sont donc visés les avocats inscrits à la liste I du tableau de l'Ordre des avocats de Luxembourg ou de Diekirch, à l'exclusion de tous les autres avocats

5 Article 40, paragraphe (8)

Le responsable du traitement dispose de trois jours pour désigner un nouveau chargé de la protection des données si la Commission nationale s'oppose à sa désignation ou à son maintien. En fait, dans la mesure où l'institution de ce chargé n'est pas une obligation pour le responsable du traitement, cette disposition prescrite par le paragraphe (8) de l'article 40 ne s'appliquera qu'en cas de refus opposé par la Commission nationale au maintien du chargé préalablement désigné.

La Commission nationale définit les modalités du contrôle continu des qualités requises à la fonction de chargé de la protection des données.

En ce qui concerne ses missions et pouvoirs, le chargé de la protection des données ne peut intervenir que pour des traitements ayant donné lieu à notification à la Commission nationale. L'article 40, paragraphe (1), précise à ce sujet que le chargé agit „dans le cadre de l'article 12, paragraphe (3) sous (a) et aux fins y visées". Il ne saurait donc intervenir dans tout traitement nécessitant une autorisation préalable de la Commission nationale, sous peine de lui voir confier un pouvoir de prendre des décisions administratives pouvant faire grief[1].

Les pouvoirs du chargé de la protection des données sont fixés au paragraphe (2) de l'article 40, à savoir:

„(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."

En cas de doute, le chargé de la protection consulte la Commission nationale quant à la conformité à la présente loi d'un traitement mis en œuvre sous sa surveillance.

L'article 12, paragraphe (3) lettre (a), précise que le chargé de la protection des données doit établir un registre des traitements effectués par le responsable du traitement qu'il surveille. Ce registre doit être continué à la Commission nationale pour permettre à celle-ci l'exercice de son pouvoir de contrôle. Les traitements mentionnés sur ce registre figureront également sur le registre public organisé par l'article 15.

*

VI. LES RECOURS JURIDICTIONNELS

Une procédure exorbitante du droit commun, l'action en cessation, a été instituée afin de faire ordonner la cessation d'un traitement mis en œuvre en violation des dispositions du présent projet de loi (B.). L'existence de cette procédure particulière ne se substitue cependant pas aux actions de droit commun (A.).

A. Les recours de droit commun

Nous avons déjà abordé les sanctions administratives qui peuvent être prises par la Commission nationale avec une possibilité de recours devant les juridictions administratives. Des sanctions pénales sont également prévues dans le projet de loi.

En ce qui concerne les recours de nature civile, l'article 38 précise clairement que l'action en cessation de l'article 39 n'est pas la seule base qu'une personne lésée par un traitement peut invoquer. Cette personne peut continuer à intenter des recours sur base du droit commun.

„En cas de dommage subi par l'utilisateur d'une base de données du chef d'information inexacte, celui-ci sera le plus souvent amené à agir en responsabilité sur la base du droit commun. En effet, le régime de responsabilité des produits défectueux institué par la directive du 25 juillet 1985 ne s'applique qu'aux dommages „physiques" causés aux personnes ou aux biens de consommation privés. Or la plupart du temps, le préjudice occasionné sera de type économique en sorte que sa réparation relève du droit commun de la responsabilité contractuelle et délictuelle. Ce dernier peut égale-

1 Doc. parl. 4735, p. 50

ment être invoqué en cas de dommage corporel étant donné que le régime de la directive ne se substitue pas, mais se superpose, aux règles de droit commun (art. 13 de la directive).“[1]

B. L’action en cessation

L’action en cessation organisée par l’article 39, paragraphe (1). Alors que le texte initial du projet de loi prévoyait une procédure devant la chambre du conseil du tribunal d’arrondissement, la commission a décidé de remplacer cette procédure par une procédure plus ancrée civilement et inspirée de l’article 21 de la loi du 27 novembre 1986 réglementant certaines pratiques commerciales et sanctionnant la concurrence déloyale.

L’action est portée devant le président du tribunal d’arrondissement du lieu où le traitement est mis en œuvre. Le président de cette juridiction peut se faire remplacer par un juge, comme en matière de référés. Contrairement à l’action en cessation de la loi du 27 novembre 1986 et à celle du projet de loi 4921 sur la protection juridique des services à accès conditionnel et des services d’accès conditionnel, l’action en cessation de l’article 39 n’est pas portée devant le président de la chambre commerciale du tribunal d’arrondissement. En effet, les droits que l’action en cessation de l’article 39 vise à protéger sont de nature civile, de sorte qu’une action devant le président du tribunal s’avère plus appropriée.

Le Procureur d’Etat peut saisir le président du tribunal d’une action en cessation lorsqu’il a déclenché une action publique pour violation de la présente loi. D’après le paragraphe (6) de l’article 39, „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 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“.

La saisine de la juridiction présidentielle intervient sur requête de la Commission nationale, lorsque le responsable du traitement ne s’est pas conformé à une sanction administrative définitive.

Enfin, la personne concernée ne peut intenter directement une action en cessation qu’après avoir d’abord saisi la Commission nationale conformément à l’article 32. Ce n’est qu’en cas d’inaction de la Commission nationale ou en cas de silence gardé par cette autorité pendant un ou trois mois, selon le cas, que la personne concernée peut elle-même agir en justice.

Le schéma de la procédure est simple. La personne concernée se plaint d’abord auprès de la Commission nationale. De deux choses l’une:

Soit la Commission nationale prend une sanction administrative à l’encontre du responsable fautif, qui peut contester cette décision devant les juridictions administratives[2]. Si ce dernier ne respecte pas la décision de la Commission nationale, alors que cette décision a été confirmée par une décision coulée en force de chose jugée ou qu’elle n’a pas été contestée en justice, la Commission nationale peut saisir le président du tribunal d’arrondissement d’une action en cessation.

Soit la Commission nationale ne prend aucune sanction ou garde le silence pendant une certaine durée, alors la personne concernée peut saisir directement la justice.

Il ne doit exister aucune différence quant à la décision à prendre par le président du tribunal d’arrondissement selon le mode de sa saisine.

Le président du tribunal d’arrondissement ordonne la cessation du traitement contraire aux dispositions du présent projet de loi et la suspension provisoire de l’activité du responsable du traitement ou du sous-traitant.

Il peut, mais ne doit pas, ordonner la fermeture provisoire de l’établissement du responsable du traitement ou du sous-traitant lorsque sa seule activité est de traiter des données. Cette fermeture provisoire visée à la dernière phrase de l’article 39, paragraphe (1) n’est que facultative. En outre, pour qu’elle puisse être prononcée, le responsable du traitement ou le sous-traitant mis en cause doit avoir pour activité exclusive le traitement de données, c’est-à-dire être un professionnel en la matière. Des „brebis

---

1 Montero, La responsabilité civile du fait des bases de données, Travaux de la Faculté de droit de Namur, Presses universitaires de Namur, p. 377, No 187. La directive du 25 juillet 1985 (JOCE du 7 août 1985, L 210/29) a été transposée en droit luxembourgeois par la loi modifiée du 21 avril 1989

2 Article 33, paragraphe (2)

galeuses“ peu respectueuses de la législation ne doivent pas noircir la réputation d'une profession respectable et des mesures draconiennes doivent être envisagées à leur encontre.

En outre, il est opportun de prévoir une sanction contre le sous-traitant, même si ce dernier, au vœu de l'article 21, ne peut procéder à un traitement que sur ordre du responsable du traitement.

Se pose la question de savoir si la fermeture provisoire de l'établissement du sous-traitant pourra être ordonnée même si ce sous-traitant effectue des traitements pour des responsables de traitement autres que le responsable contrevenant. D'après le texte de l'article 39, la fermeture provisoire pourra être ordonnée en pareille hypothèse. Certes le sous-traitant agit sous les ordres du responsable du traitement, mais il a une obligation de veiller à la légalité du traitement et devra s'opposer à des instructions du responsable du traitement, lorsqu'il estime que ces instructions débouchent sur un traitement contrevenant aux dispositions légales ou réglementaires.

Du point de vue procédural, comme dans le cadre de la loi précitée du 27 novembre 1986, 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.

Le paragraphe (2) reprend la jurisprudence édictée sous l'empire de l'article 21 de la loi du 27 novembre 1986 qui admet la recevabilité de l'action en cessation „même lorsque le traitement illégal a pris fin ou n'est plus susceptible de se reproduire“.[1]

Le président du tribunal d'arrondissement peut assortir sa décision d'une astreinte sur base des articles 2059 à 2066 du Code civil.

Il peut ordonner la publication de sa décision, soit en totalité soit par extrait, aux frais du contrevenant. La publication peut être ordonnée par la voie des journaux ou de toute autre manière. Elle ne peut avoir lieu qu'en vertu d'une décision coulée en force de chose jugée, c'est-à-dire après que les délais d'appel aient passé ou qu'un appel ait été vidé. On tempère ainsi les effets de la décision du président du tribunal qui est exécutoire par provision.

Cette procédure va permettre de prendre, dans un délai rapide, des mesures importantes pour le respect des droits et libertés fondamentales de la personne concernée.

*

VII. LE TRANSFERT DE DONNEES VERS UN PAYS TIERS

Les articles 18 et 19 régissent les transferts de données vers des Etats non membres de l'Union européenne.

Le projet de loi sous rubrique reprend les dispositions figurant aux articles 25 et 26 de la directive. L'article 18 fixe les principes régissant les flux transfrontaliers en direction de pays tiers (A.), tandis que l'article 19 réunit les dérogations (B.).

A. Principes

Il aurait été aberrant d'affirmer haut et fort que la directive tend à l'établissement d'un „niveau élevé de protection dans la Communauté“[2] tout en ne tenant pas compte des mouvements internationaux de données et du caractère insatisfaisant d'une protection des personnes concernées dans le pays de destination.

C'est pourquoi le transfert de données vers un pays tiers „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“[3]. Peu importe que les données aient déjà fait l'objet d'un traitement avant leur transfert ou qu'elles aient été collectées en vue d'un traitement dans un Etat tiers.

Par conséquent, comme le relève l'article 18, paragraphe (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“.

---

1 Cour 19 octobre 1977, Pas. 24, 46, Cour 31 mai 1978, Pas. 24, 127

2 Directive, considérant 10

3 Article 18, paragraphe (1)

Les flux de données entre plusieurs Etats membres de l'Union européenne ne sont pas concernés[1].

En outre seul l'Etat de la destination finale est pris en compte. Ainsi, si les données collectées au Luxembourg sont d'abord transférées en France, puis aux Etats-Unis, enfin au Canada, le niveau de protection qui sera considéré sera celui existant au Canada.

Qu'est-ce qu'un „niveau de protection adéquat"?

> „Ce qui est visé n'est effectivement pas une concurrence „équivalente" dans le sens où un recopiage mot à mot de la directive serait suffisant: il s'agit bien de vérifier comment, en pratique, les principes fondamentaux de protection des données sont respectés dans les pays tiers (principe de similarité fonctionnelle)."[2]

Pour vérifier ceci, le responsable du traitement doit tenir compte „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].

Le groupe prévu à l'article 29 de la directive a établi une méthodologie et des critères d'appréciation du caractère adéquat de la protection[4]. Le responsable du traitement peut légitimement s'inspirer de ces critères.

En cas de doute, il peut saisir la Commission nationale. Ce sera elle qui appréciera si un pays tiers assure un niveau de protection adéquat[5]. La Commission nationale informe la Commission européenne des pays au sujet desquels elle a constaté l'absence d'un niveau de protection adéquat[6].

L'article 25, paragraphe 6., de la directive permet à la Commission européenne de constater qu'un pays tiers assure un niveau de protection adéquat. L'alinéa 2 ajoute que „les Etats membres prennent les mesures nécessaires pour se conformer à la décision de la Commission [européenne]".

Donc si la Commission européenne constate qu'un Etat assure un niveau de protection adéquat des personnes, un transfert de données en direction de ce pays ne pose pas de problème.

La Commission européenne a reconnu que les législations suisse, hongroise et canadienne présentaient un niveau de protection adéquat[7]. De même, en vertu d'une décision de la Commission européenne du 26 juillet 2000, la Commission a décidé que les principes de la „sphère de sécurité/safe harbour" édictés par le ministère américain du commerce remplissent les critères de protection adéquate[8]. Si une société américaine respecte les principes de la „sphère de sécurité" et adhère au contrat y relatif, elle peut importer des données en provenance, même indirecte, d'un Etat membre de l'Union européenne[9].

B. Exceptions

L'article 19 permet dans certaines hypothèses le transfert de données dans un pays tiers qui n'assure pas un niveau de protection adéquat.

Un transfert est possible dans les situations suivantes, reprises telles quelles de l'article 26 de la directive:

a. la personne concernée a donné son consentement au transfert envisagé,

---

1 Havelange, Lacoste, op. cit., p. 243

2 Havelange, Lacoste, op. cit., p. 242

3 Article 18, paragraphe (2).

4 Document de travail adopté le 24 juillet 1998; publié sous: www.europa.eu.int/comm/ internal_market/en/dataprot/wpdocs/index.htm

5 Voir article 18, paragraphe (4)

6 L'article 20 institue un mécanisme d'information réciproque entre les autorités luxembourgeoises et la Commission européenne

7 Voir Commission européenne, communiqué de presse du 22 janvier 2002

8 Pour une description de cette décision: Havelange, Lacoste, op. cit., pp. 244 et ss.

9 Pour la liste de ces sociétés: http://web.ita.doc.gov/safeharbour/shlist.nsf/webPages/safe+harbour+list

b. le transfert est 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,

c. le transfert est 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,

d. le transfert est 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,

e. le transfert est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou

f. le transfert intervient depuis un registre public tel que prévu à l'article 12, paragraphe (3) lettre (b).

Le responsable du traitement doit notifier à la Commission nationale un rapport établissant les conditions dans lesquelles il a opéré le transfert vers un pays tiers qui ne satisfait pas au critère de la protection adéquate.

Mais, conformément au paragraphe (3) de l'article 19, „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".

La Commission européenne a adopté des décisions établissant des clauses-types afin de simplifier la procédure de ceux qui souhaitent transférer des données tout en voulant s'assurer d'un niveau de protection le plus élevé possible[1]. Si les clauses ne sont pas obligatoires pour les sociétés, il s'agit néanmoins d'un instrument pratique afin de se conformer aux prescriptions du paragraphe (3) de l'article 19.

*

VIII. DISPOSITIONS PENALES

Les prescriptions légales les plus importantes sont sanctionnées pénalement. Il n'est pas nécessaire d'entrer dans le détail de toutes ces dispositions.

Contentons-nous des quelques remarques suivantes.

D'abord, la grande majorité des infractions sont des infractions matérielles. L'utilisation dans certains cas de l'adverbe „sciemment" dénote l'exigence d'une intention doleuse et sert à les distinguer des infractions matérielles à l'endroit desquelles cet adverbe n'a pas été inséré. C'est le cas des articles 28, paragraphes (2) et (8), 30, paragraphe (2), et 32, paragraphe (11).

Ensuite, les sanctions prévues pour toutes les infractions sont uniformes, à savoir un emprisonnement de huit jours à un an et/ou une amende de 251 à 125.000 euros. Ceci laisse à la juridiction répressive suffisamment de latitude pour trouver la sanction adéquate. La juridiction répressive peut en outre pour chaque infraction ordonner la cessation du traitement. Cette cessation peut être assorti d'une astreinte, sauf à l'endroit des articles 28, paragraphe (2) et (8), 29, paragraphe (5), 30, paragraphe (2), et 32, paragraphe (1). Ces dispositions „traitent en effet respectivement du droit d'accès et du droit d'opposition de la personne concernée ou encore des missions et pouvoirs de la Commission nationale, matière où il paraît difficile de concevoir le traitement illégal à faire cesser et sanctionner moyennant peine d'astreinte".[2]

Enfin, les articles 8, paragraphe (4) et 17, paragraphe (3), précisent que ne sont visées que les personnes „agissant à titre privé". Il faut éviter que les forces de l'ordre soient exposées à des sanctions pénales, si elles agissent en dehors du cadre réglementaire. La sanction pénale devra, à l'évidence, être limitée aux personnes agissant à titre particulier, la surveillance des forces de l'ordre étant assurée par l'autorité de contrôle et les activités des agents relevant du contrôle interne.

*

1 Voir décisions de la Commission 2001/491/CE et 2002/17/CE

2 Deuxième avis complémentaire du Conseil d'Etat, doc. parl. 4735[12]

IX. UNE DISPOSITION SPECIFIQUE ET EXCEPTIONNELLE: L'ARTICLE 41

La commission partage entièrement le constat que „suite à la libéralisation des télécommunications la présence sur le marché d'une multitude d'opérateurs et de fournisseurs de services a rendu de plus en plus difficile l'identification et la localisation d'une personne pour l'accomplissement d'une mission légale de surveillance (…) ou d'une mission de sauvegarde de la vie humaine par les services de secours"[1].

S'inspirant de la législation néerlandaise, et afin d'éviter que les autorités et services de secours n'aient chaque fois à contacter chaque opérateur et fournisseur de services, l'article 41 permet, dans des conditions strictes, à certaines autorités et services d'obtenir un certain nombre de renseignements sur les abonnés et utilisateurs de ces opérateurs et fournisseurs.

L'article 41, paragraphe (1), énumère les conditions d'accès à ces données.

Les autorités compétentes visées aux articles 88-1 à 88-4 du code d'instruction criminelle et celles agissant dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du code d'instruction criminelle peuvent demander à l'Institut Luxembourgeois de régulation („ILR") d'avoir accès 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.

Ces autorités et la centrale n'ont accès qu'aux données relatives à l'identité des abonnés et utilisateurs, à savoir nom, prénoms, adresse et, le cas échéant, l'adresse IP.

L'accès se fait de plein droit et sur requête à adresser à l'ILR.

La centrale des secours d'urgence 112 et la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg[2] accèdent dans les mêmes conditions et modalités que les autorités visées ci-dessus aux seules données concernant l'identité des abonnés et utilisateurs des opérateurs et fournisseurs de communications électroniques. Elles n'ont pas accès aux données des services postaux. La commission ne voit en effet pas l'utilité d'accès à ces données étant entendu que seule une situation d'urgence justifie une demande d'accès émanant desdites centrales.

Une nouvelle fois le principe de finalité gouverne l'accès à ces données. „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 et de la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg."[3]

Pour permettre cet accès, l'article 41, paragraphe (2) oblige les opérateurs et les fournisseurs à mettre d'office et gratuitement à la disposition de l'ILR les données en question. Ce paragraphe continue comme suit: „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."

La procédure est entièrement automatisée après autorisation de la Commission nationale. Celle-ci vérifie en particulier la sécurisation du système informatique utilisé. Cette automatisation permettra l'accès à distance par voie de communication électronique.[4]

La précision de l'automatisation s'avère indispensable du fait qu'un traitement „manuel" d'une requête soumise par fax ou lettre:

a. présuppose du côté de l'ILR la mise en place d'un dispositif supplémentaire en matière de ressources humaines, et

---

1 Doc. parl. 4735, p. 51

2 La centrale du service d'incendie et de sauvetage de la Ville de Luxembourg a été ajoutée au motif que ses activités sont similaires voire identiques à celle de la centrale des secours d'urgence 112.

3 Article 41, paragraphe (3)

4 Article 41, paragraphe (4)

b. crée un problème de responsabilité dans le chef de l'ILR du fait que celui-ci serait amené à apprécier l'origine et l'exactitude de ces requêtes ce qui n'est pas son rôle. L'esprit de l'article 41 est d'offrir un outil technique destiné à avoir plus facilement accès au nom de la personne et à son numéro de téléphone (IP adresse …) nonobstant les procédures déclenchées préalablement. L'ILR n'est qu'un interface entre opérateurs et données.

*

X. DISPOSITIONS TRANSITOIRES ET FINALES; ENTREE EN VIGUEUR

Au vœu de l'article 45, la loi entrera en vigueur le premier jour du quatrième mois qui suit sa publication au Mémorial. Cependant, afin de permettre la mise en place de la Commission nationale le plus rapidement possible, il est prévu que les dispositions régissant l'organisation de celle-ci entrent en vigueur trois jours après publication de la loi au Mémorial.

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

Cependant „pour autant qu'ils ne sont pas contraires aux dispositions de la présente loi, les règlements pris en exécution de la loi modifiée du 31 mars 1979 précitée resteront en vigueur tant qu'ils n'auront pas été remplacés par de nouvelles dispositions"[1]. Il s'agit de combler le vide juridique qui résulterait d'une abrogation expresse des règlements grand-ducaux pris en exécution de la loi modifiée du 31 mars 1979. Les règlements d'exécution, trouvant une base légale suffisante dans le nouveau texte, resteront en vigueur jusqu'à ce qu'il est pourvu à leur remplacement par de nouvelles dispositions. Sont plus particulièrement visés:

– le règlement grand-ducal du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale, pris sur base de l'article 12-1 de la loi de 1979;
– le règlement grand-ducal du 2 octobre 1992 réglementant l'utilisation de données nominatives médicales dans les traitements informatiques; et
– le règlement grand-ducal du 9 août 1993 autorisant la création et l'exploitation d'une banque de données nominatives constituant la partie nationale du système d'information Schengen (N. SIS) dont la base légale est encore constituée par la loi du 3 juillet 1992 portant approbation des accords de Schengen.

La commission n'a pas retenu le régime transitoire proposé par le Conseil d'Etat. Le régime transitoire du projet de loi lui apparaît plus adapté, alors que la loi du 31 mars 1979 doit être abrogée dans son entierté.

En vertu de l'article 42, paragraphe (1), les responsables du traitement auront deux ans à compter de l'entrée en vigueur de la loi à venir pour conformer les traitements existant dans des fichiers non automatisés ou automatisés antérieurs à ladite entrée en vigueur aux dispositions du chapitre II[2] et du chapitre VI[3]. Le dernier paragraphe de l'article 42 prévoit une exception en ce qui concerne les données conservées uniquement à des fins de recherches historiques. Dans ce cas, une décision devra être prise par la Commission nationale.

Les fichiers visés à l'article 42, paragraphe (1), sont ceux qui auront été autorisés sous l'empire de la loi du 31 mars 1979. Le projet de loi ne vise en effet pas à „régulariser" des banques de données qui n'auraient, malgré l'obsolescence de cette législation et malgré la philosophie différente du projet de loi, pas été autorisées. Au cas où des banques de données n'auraient pas été autorisées, les responsables du traitement devront procéder à la notification, voire demander l'autorisation préalable, pour les traitements en cause.

La personne concernée peut cependant demander à obtenir avant l'expiration de ce délai biennal, notamment dans le cadre de 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[4].

---

1 Article 45

2 Chapitre intitulé „Conditions de licéité du traitement", articles 4 à 11

3 Chapitre intitulé „Droits de la personne concernée", articles 26 à 31

4 Article 42, paragraphe (2)

En vue de la mise en vigueur des dispositions transitoires de l'article 42, l'article 43 prévoit que le schéma de notification prévu à l'article 13, paragraphe (3), devra être établi par la Commission nationale dans les quatre mois de la nomination de ses membres. La date à partir de laquelle ce schéma de notification est disponible auprès de la Commission nationale sera publiée au Mémorial et fera l'objet d'un communiqué de presse aux journaux édités au Luxembourg.

A partir de cette date, les responsables du traitement auront quatre mois pour notifier leurs traitements à la Commission nationale. En vertu du paragraphe (4), le délai de quatre mois est porté à douze mois en ce qui concerne les traitements non automatisés de données contenues ou appelées à figurer dans un fichier.

La commission tient à préciser qu'en cas de discordance entre les dates de publication au Mémorial et dans les journaux, ce sera la date de publication au Mémorial qui fera courir le délai de quatre mois.

Le paragraphe (3) de l'article 43 concerne les traitements autorisés en application de la loi du 31 mars 1979 par règlement grand-ducal ou arrêté ministériel „autorisant la création et l'exploitation d'une banque de données". Les responsables de tels traitements notifieront ou demanderont l'autorisation de leurs traitements à l'expiration de la durée de validité de l'autorisation octroyée, à moins que pour des raisons de conformité avec les dispositions du projet de loi, ils jugent nécessaire de le faire auparavant.

*

CONCLUSION

Au vu de l'expérience malheureuse de la pratique de la loi du 31 mars 1979, le législateur a saisi l'occasion de la transposition de la directive pour réformer de fond en comble la législation relative à la protection des données.

L'intention du législateur a été d'édicter une législation réaliste visant à établir une balance entre les intérêts des responsables du traitement et les droits et libertés fondamentales des personnes concernées.

D'aucuns reprochent au projet de loi l'utilisation de termes vagues et son caractère „fourre-tout".

La flexibilité nécessaire dans cette matière et les termes utilisés dans la directive ont parfois donné naissance à des termes aux contours certes vagues. Il est en effet difficile de prévoir la portée de l'évolution technologique en la matière. A-t-on d'ailleurs jamais regretté les termes utilisés par exemple à l'endroit des articles 1382 à 1384 du Code civil ou de l'article 496 du Code pénal?

Le respect des libertés et droits fondamentaux commande à regrouper au sein d'un seul texte de loi l'ensemble des dispositions relatives à la protection des personnes à l'égard des traitements de données, même si la transposition de la directive 97/66/EE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications fera l'objet d'un projet de loi séparé.

*

Compte tenu des remarques qui précèdent, la commission invite la Chambre des Députés à voter le projet de loi dans la teneur suivante:

*

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

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

Art. 1er. – ***Objet***

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 et fait respecter les intérêts légalement protégés des personnes morales.

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;

(c) „consentement de la personne concernée": toute manifestation de volonté expresse, non équivoque, 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;

(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 ou morale est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique;

(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;

(j) „interconnexion": toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d'autres responsables du traitement;

(k) „ministre": le ministre ayant dans ses attributions la protection des données;

(l) „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, ainsi que des prestations familiales ou d'aides sociales;

(m) „pays tiers": Etat non membre de l'Union européenne;

(n) „personne concernée": toute personne physique ou morale, publique ou privée ou groupement de fait, qui fait l'objet d'un traitement de données à caractère personnel;

(o) „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;

(p) „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;

(q) „surveillance": 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;

(r) „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;

(s) „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***

(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.

(2) Sont soumis à la présente loi:

(a) le traitement mis en oeuvre par un responsable du traitement soumis au droit 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 s'applique 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.

(4) La présente loi s'applique à toute forme de captage, de traitement et de diffusion de sons et images qui permettent d'identifier des personnes physiques ou morales.

(5) 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

– au traitement de données concernant une personne morale et dont la publication est prescrite par une loi ou un règlement.

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.

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

(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*

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

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

(b) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, ou si

(c) le traitement 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 si

(d) le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, ou si

(e) le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou si

(f) 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:

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

(b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement notamment 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 oeuvre, 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

(f) le traitement mis en oeuvre conformément aux règles de procédures judiciaires en matière civile applicables est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice s'il est mis en oeuvre à cette fin exclusive, 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 et que ce traitement est mis en oeuvre conformément au régime d'autorisation préalable de la Commission nationale tel que prévu à l'article 14, ou lorsque

(h) le traitement est mis en oeuvre par voie de règlement grand-ducal tel que prévu à l'article 17.

(3) L'article 6 paragraphe (1) ne s'applique pas lors d'une procédure judiciaire ou d'une enquête pénale. Toutefois les données génétiques ne peuvent être traitées que 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.

(4) Par dérogation à l'article 6, paragraphe (1), les données génétiques ne peuvent faire l'objet d'un traitement que:

(a) dans les cas visés par les articles 6, paragraphe (2) lettres (c), (f), (g), (h), 6 paragraphe (3) et 7 de la présente loi, ou lorsque

(b) la personne concernée a donné son consentement et si le traitement est effectué dans les seuls domaines de la santé ou de la recherche scientifique sauf indisponibilité du corps humain et 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.

(5) 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***

(1) Lorsque le traitement de données tel que défini à l'article 6 paragraphe (1) de la présente loi est 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, de la recherche scientifique dans le domaine de la biologie et de la médecine, le traitement de ces données peut être mis en oeuvre 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 oeuvrant dans les domaines social, familial et thérapeutique, désignées par règlement grand-ducal. Le recours à un sous-traitant est possible dans les conditions prévues à l'article 21.

(2) Le traitement visé ci-dessus fait l'objet d'une autorisation préalable de la Commission nationale.

(3) Par dérogation au paragraphe (2) qui précède sont soumis à notification:

– le traitement mis en oeuvre conformément à l'article 36 de la loi du 28 août 1998 sur les établissements hospitaliers;
– le traitement mis en oeuvre par un médecin et concernant ses patients.

(4) 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.

(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***

(1) Sans préjudice des dispositions prévues dans la législation sur la liberté dans les moyens de communication de masse 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 oeuvre 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;

lorsque le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou à des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée:

(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;

(e) au droit d'accès de la personne concernée qui peut être différé ou limité conformément à l'article 28, paragraphe (4) et à l'article 29.

(2) Lors de la notification d'un traitement effectué à des fins de journalisme ou d'expression artistique ou littéraire, la notification ne renseigne que sur le(s) nom(s) et adresse(s) du responsable du traitement ou de son représentant.

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 à la sécurité des usagers ainsi qu'à la prévention des accidents, ou

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

(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 oeuvre 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,

(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. – ***Traitement à des fins de surveillance sur le lieu du travail***

(1) Le traitement à des fins de surveillance sur le lieu de travail peut être mis en oeuvre, conformément à l'article 14, par l'employeur s'il en est le responsable. Un tel traitement n'est possible que s'il est nécessaire:

(a) pour les besoins de sécurité et de santé des travailleurs, ou

(b) pour les besoins de protection des biens de l'entreprise, ou

(c) pour le contrôle du processus de production portant uniquement sur les machines, ou

(d) pour le contrôle temporaire de production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte, ou

(e) dans le cadre d'une organisation de travail selon l'horaire mobile conformément à la loi.

Dans les cas visés aux lettres (a), (d) et (e), le comité mixte d'entreprise, le cas échéant institué, a un pouvoir de décision tel que défini à l'article 7, paragraphes (1) et (2), de la loi modifiée du 6 mai 1974 instituant des comités mixtes dans les entreprises du secteur privé et organisant la représentation des

salariés dans les sociétés anonymes. Le consentement de la personne concernée ne rend pas légitime le traitement mis en oeuvre par l'employeur.

(2) Sans préjudice du droit à l'information de la personne concernée 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.

(3) Quiconque effectue un traitement en violation des dispositions du présent article est puni d'une peine d'emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une des 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 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.

(2) Pour les traitements des données dont la mise en œuvre n'est pas susceptible de porter atteinte aux libertés et droits fondamentaux, et notamment à la vie privée, des personnes concernées, la Commission nationale établit et publie des directives en vue d'une notification simplifiée.

Ces directives précisent:

(a) la ou les finalités du traitement faisant l'objet d'une notification simplifiée;
(b) la ou les catégories de données traitées;
(c) la ou les catégories de personnes concernées;
(d) les destinataires ou catégories de destinataires auxquels les données sont communiquées;
(e) la durée de conservation.

Les traitements qui correspondent à ces directives font l'objet d'une notification simplifiée de conformité envoyée à la Commission nationale le cas échéant par voie électronique.

(3) Est exempté de l'obligation de notification:

(a) le responsable du traitement qui désigne un chargé de la protection des données tenu notamment d'assurer, de manière indépendante, l'application des dispositions légales en la matière et d'établir et de continuer à la Commission nationale un registre des traitements effectués par le responsable du traitement conformément aux dispositions relatives à la publicité des traitements telles que prévues à l'article 15;
(b) le traitement ayant pour seul objet 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) le traitement mis en œuvre conformément aux règles de procédures judiciaires en matière civile et nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice.

(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:

(a) le nom et l'adresse du responsable du traitement, et le cas échéant de son représentant et du sous-traitant;

(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;

(h) la durée de conservation des données.

(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.

(3) La notification se fait auprès de la Commission nationale moyennant support papier ou informatique suivant un schéma à établir par elle. Il est accusé réception de la notification.

(4) Un règlement grand-ducal fixera le montant et les modalités de paiement d'une redevance à percevoir lors de toute notification et de toute modification de notification.

Art. 14. – ***Autorisation préalable de la Commission nationale***

(1) Sont soumis à l'autorisation préalable de la Commission nationale:

(a) les traitements prévus aux articles 6, paragraphe (2) lettres (a), (b), (e), (g), 6 paragraphe (4) lettre (b), aux articles 7, paragraphe (1), 10 et 11 de la présente loi;

(b) les traitements de données à des fins historiques, statistiques ou scientifiques visés à l'article 4, paragraphe (2). La Commission nationale vérifie en particulier si ces traitements ne peuvent être réalisés sur base de données rendues anonymes;

(c) l'interconnexion de données visée à l'article 16;

(d) le traitement concernant le crédit et la solvabilité des personnes concernées;

(e) 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.

(2) La demande d'autorisation comprend les informations suivantes:

(a) le nom et l'adresse du responsable du traitement ou de son représentant et le cas échéant du sous-traitant;

(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 aux articles 22 et 23;

(j) la durée de conservation des données.

(3) 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 autorisés 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.

(4) 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

(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 (3) (a).

(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,

(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 de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi,

(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***

(1) L'interconnexion de données qui n'est pas expressément prévue par un texte légal doit faire l'objet d'une autorisation préalable de la Commission nationale sur demande conjointe présentée par les responsables des traitements en cause.

(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.

(3) L'interconnexion n'est autorisée que dans le respect des finalités identiques ou liées de fichiers et 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'Organisations internationale de police criminelle (OIPC – Interpol).

(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 ci-dessus.

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

(f) le transfert intervienne depuis un registre public tel que prévu à l'article 12, paragraphe (3) lettre (b).

(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 notifier à la Commission nationale un rapport établissant les conditions dans 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***

(1) La Commission nationale informe le ministre de toute décision prise en application de l'article 18, paragraphes (3) et (4), et de l'article 19, paragraphes (1) et (2). Le ministre en informe la Commission européenne.

(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***

(1) Le responsable du traitement doit mettre en œuvre toutes les mesures techniques et d'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. Ces mesures font l'objet d'un rapport annuel à soumettre par le responsable du traitement 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.

(4) Le responsable du traitement agissant dans le cadre de l'accomplissement de ses missions visées à l'article 7, paragraphe (1), 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;
- la durée de conservation 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;
- la durée de conservation 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;

(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 de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi;

(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,

(2) Les dispositions de l'article 26 sont susceptibles de dérogations lors de la collecte de données dans les conditions prévues à l'article 9, paragraphe (1) lettre (c).

(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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article.

(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.

(4) Toute personne a un droit d'accès aux données la concernant et utilisées aux fins d'un traitement mis en oeuvre dans le cadre de la liberté d'expression tel que prévu à l'article 9. Aussi longtemps que les données auxquelles l'accès est demandé n'ont pas été publiées, la communication de ces données, ainsi que toute information disponible sur leur origine ne peut se faire que par l'intermédiaire de la Commission nationale.

(5) 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.

(6) 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.

(7) Toute rectification, tout effacement ou verrouillage effectué conformément au paragraphe (5) 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.

(8) Sans préjudice de la sanction prévue au paragraphe (5), 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article.

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;

(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 de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi;

(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 et que la mesure d'exception est prise conformément à l'article 28, paragraphe (4);

(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).

(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.

(3) 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.

(4) 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.

(5) Quiconque contrevient à la disposition du paragraphe (3) 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 (3) du présent article.

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 oeuvre par le responsable du traitement ne peut pas porter sur ces données;

(b) de s'opposer, sur demande et gratuitement, au traitement la concernant envisagé par le responsable du traitement 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article.

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 oeuvre 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 oeuvre des traitements soumis au régime de l'article 14 de la présente loi;

(e) être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi. Ces avis sont publiés au rapport annuel visé à l'article 15, paragraphe (6);

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

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

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

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

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

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

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

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

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

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

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

(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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article.

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.

En cas de cessation du mandat, il est réintégré sur sa demande dans son administration d'origine à un emploi correspondant au traitement qu'il a touché précédemment, augmenté des échelons et majorations de l'indice se rapportant aux années de service passées comme président ou membre effectif jusqu'à concurrence du dernier échelon du grade.

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***

(1) Le cadre du personnel de la Commission nationale comprend les fonctions et emplois suivants:

Dans la carrière moyenne de l'administration, grade de computation de la bonification d'ancienneté: grade 7, carrière du rédacteur:

- des inspecteurs principaux 1er en rang
- des inspecteurs principaux
- des inspecteurs
- des chefs de bureau
- des chefs de bureau adjoints
- des rédacteurs principaux
- des rédacteurs

Les agents de la carrière moyenne des rédacteurs sont des fonctionnaires de l'Etat en ce qui concerne notamment leur statut, leur traitement et leur régime de pension qui est régi par les dispositions légales régissant les 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.

(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 à l'article 13 de la présente loi. Pour le solde des frais restant à couvrir dans le cadre de ses missions conférées par la présente loi, la Commission nationale bénéficiera d'une dotation d'un montant à déterminer sur une base annuelle et à inscrire au budget de l'Etat.

(5) La loi du 27 novembre 2001 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2002 est modifiée comme suit: il est ajouté au budget des dépenses au Chapitre III – Dépenses courantes sous „00 – Ministère d'Etat" une section „00.9 Commission nationale pour la protection des données" émargeant les articles suivants:

„12.300:	Prise en charge par l'Etat des frais encourus par la Commission nationale pour la protection des données. (crédit non limitatif et sans distinction d'exercice)	200.870
33.000:	Dotation initiale en faveur de la Commission nationale pour la protection des données	200.000"

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*

(1) Tout responsable de traitement peut, dans le cadre de l'article 12, paragraphe (3) sous (a), et aux fins y visées, 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.

(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:

(a) il ne connaît aucun lien de subordination vis-à-vis du responsable du traitement et ne peut être lié au responsable du traitement par un contrat de travail:

(b) il ne peut être révoqué pour des raisons liées à l'exercice de ses missions, hormis le cas de la violation de ses obligations légales ou conventionnelles.

(4) Le chargé de la protection 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.

(5) 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.

(6) 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 ainsi que d'assises financières d'une valeur de 20.000 euros.

(7) 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.

(8) La Commission nationale vérifie les qualités de tout chargé de la protection des données.

Elle peut s'opposer à tout moment à la désignation ou au maintien du chargé de la protection des données lorsqu'il:

(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.

(9) La Commission nationale définit les modalités du contrôle continu des qualités requises à la fonction de chargé de la protection des données.

(10) 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 (ci-après „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.

La centrale des secours d'urgence 112 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.

(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 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.

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).

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.

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.

Luxembourg, le 10 juillet 2002

Le Président,
Laurent MOSAR

Le Rapporteur,
Patrick SANTER

Service Central des Imprimés de l'Etat

4735/14

N° 4735[14]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

* * *

DISPENSE DU SECOND VOTE CONSTITUTIONNEL PAR LE CONSEIL D'ETAT

(19.7.2002)

Le Conseil d'Etat,

appelé par dépêche du Premier Ministre, Ministre d'Etat, du 18 juillet 2002 à délibérer sur la question de dispense du second vote constitutionnel du

PROJET DE LOI

relatif à la protection des personnes à l'égard du traitement des données à caractère personnel

qui a été adopté par la Chambre des députés dans sa séance du 17 juillet 2002 et dispensé du second vote constitutionnel;

Vu ledit projet de loi et les avis émis par le Conseil d'Etat en ses séances des 29 janvier 2002 et 2 juillet 2002 et 9 juillet 2002;

se déclare d'accord

avec la Chambre des députés pour dispenser le projet de loi en question du second vote prévu par l'article 59 de la Constitution.

Ainsi décidé en séance publique du 19 juillet 2002.

Le Secrétaire général,
Marc BESCH

Le Président,
Marcel SAUBER

Service Central des Imprimés de l'Etat

Document écrit de dépot

I-2001-O-M-2602-01(1459)

Dépôt: Mme Simone BEISSEL
17 juillet 2002

1

pl 4735

MOTION

La Chambre des Députés,

- constatant que les progrès en informatique, aussi bénéfiques qu'ils soient, recèlent également des dangers;

- considérant que l'objectif du projet de loi relatif à la protection des personnes à l'égard du traitement des données à caractère personnel est d'endiguer les risques d'abus;

- considérant le degré de complexité élevé des dispositions retenues dans le projet de loi susmentionné;

- soulignant les incidences du projet de loi sous rubrique sur le fonctionnement des institutions et des organismes publics ainsi que sur toute personne privée ou morale procédant au traitement de données à caractère personnel;

- relevant les répercussions que le traitement de données à caractère personnel peut avoir sur les droits et libertés des personnes dont les données font l'objet d'un traitement;

- considérant qu'un des principes clés dudit projet de loi est de garantir l'information des personnes dont les données sont traitées afin de s'assurer du consentement éclairé de ces dernières;

invite le Gouvernement,

- à faire élaborer une brochure relatant en des termes simples et compréhensibles les tenants et aboutissants de cette nouvelle loi et informant les citoyens sur leurs droits et devoirs en la matière;

- à s'assurer de la diffusion la plus large possible de cette brochure et à faire en sorte qu'elle soit rendue accessible aux internautes sur le site internet du gouvernement.

P. Sauber F. Greisen R Garcia A. Bodry

L. Mosar

4735

MEMORIAL
Journal Officiel
du Grand-Duché de
Luxembourg

MEMORIAL
Amtsblatt
des Großherzogtums
Luxemburg

RECUEIL DE LEGISLATION

A — N° 91 13 août 2002

Sommaire

PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel . . . . . page 1836

Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau;

Notre Conseil d'Etat entendu;

De l'assentiment de la Chambre des Députés;

Vu la décision de la Chambre des Députés du 17 juillet 2002 et celle du Conseil d'Etat du 19 juillet 2002 portant qu'il n'y a pas lieu à second vote;

Avons ordonné et ordonnons:

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

Art. 1er. Objet

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 et fait respecter les intérêts légalement protégés des personnes morales.

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;

(c) "*consentement de la personne concernée*": toute manifestation de volonté expresse, non équivoque, 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;

(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 ou morale est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique;

(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;

(j) "*interconnexion*": toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d'autres responsables du traitement;

(k) "*ministre*": le ministre ayant dans ses attributions la protection des données;

(l) "*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, ainsi que des prestations familiales ou d'aides sociales;

(m) "*pays tiers*": Etat non membre de l'Union européenne;

(n) "*personne concernée*": toute personne physique ou morale, publique ou privée ou groupement de fait, qui fait l'objet d'un traitement de données à caractère personnel;

(o) *"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;

(p) *"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;

(q) *"surveillance"*: 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;

(r) *"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;

(s) *"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

(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.

(2) Sont soumis à la présente loi:

(a) le traitement mis en œuvre par un responsable du traitement soumis au droit 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 s'applique 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.

(4) La présente loi s'applique à toute forme de captage, de traitement et de diffusion de sons et images qui permettent d'identifier des personnes physiques ou morales.

(5) 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,
- au traitement de données concernant une personne morale et dont la publication est prescrite par une loi ou un règlement.

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.

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

(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

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

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

(b) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, ou si

(c) le traitement 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 si

(d) le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, ou si

(e) le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou si

(f) 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:

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

(b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement notamment 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

(f) le traitement mis en œuvre conformément aux règles de procédures judiciaires applicables en matière civile est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice s'il est mis en œuvre à cette fin exclusive, 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 et que ce traitement est mis en œuvre conformément au régime d'autorisation préalable de la Commission nationale tel que prévu à l'article 14, ou lorsque

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

(3) L'article 6 paragraphe (1) ne s'applique pas lors d'une procédure judiciaire ou d'une enquête pénale. Toutefois les données génétiques ne peuvent être traitées que 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.

(4) Par dérogation à l'article 6, paragraphe (1), les données génétiques ne peuvent faire l'objet d'un traitement que:

(a) dans les cas visés par les articles 6, paragraphe (2) lettres (c), (f), (g), (h), 6 paragraphe (3) et 7 de la présente loi, ou lorsque

(b) la personne concernée a donné son consentement et si le traitement est effectué dans les seuls domaines de la santé ou de la recherche scientifique sauf indisponibilité du corps humain et 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.

(5) 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

(1) Lorsque le traitement de données tel que défini à l'article 6 paragraphe (1) de la présente loi est 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, de la recherche scientifique dans le domaine de la biologie et de la médecine, le traitement de ces données 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, désignées par règlement grand-ducal. Le recours à un sous-traitant est possible dans les conditions prévues à l'article 21.

(2) Le traitement visé ci-dessus fait l'objet d'une autorisation préalable de la Commission nationale.

(3) Par dérogation au paragraphe (2) qui précède sont soumis à notification:

- le traitement mis en œuvre conformément à l'article 36 de la loi du 28 août 1998 sur les établissements hospitaliers;
- le traitement mis en œuvre par un médecin et concernant ses patients.

(4) 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.

(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

(1) Sans préjudice des dispositions prévues dans la législation sur la liberté dans les moyens de communication de masse 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;

lorsque le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou à des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée;

(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;

(e) au droit d'accès de la personne concernée qui peut être différé ou limité conformément à l'article 28, paragraphe (4) et à l'article 29.

(2) Lors de la notification d'un traitement effectué à des fins de journalisme ou d'expression artistique ou littéraire, la notification ne renseigne que sur le(s) nom(s) et adresse(s) du responsable du traitement ou de son représentant.

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 à la sécurité des usagers ainsi qu'à la prévention des accidents, ou

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

(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. Traitement à des fins de surveillance sur le lieu du travail

(1) Le traitement à des fins de surveillance sur le lieu de travail peut être mis en œuvre, conformément à l'article 14, par l'employeur s'il en est le responsable. Un tel traitement n'est possible que s'il est nécessaire:

(a) pour les besoins de sécurité et de santé des travailleurs, ou

(b) pour les besoins de protection des biens de l'entreprise, ou

(c) pour le contrôle du processus de production portant uniquement sur les machines, ou

(d) pour le contrôle temporaire de production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte, ou

(e) dans le cadre d'une organisation de travail selon l'horaire mobile conformément à la loi.

Dans les cas visés aux lettres (a), (d) et (e), le comité mixte d'entreprise, le cas échéant institué, a un pouvoir de décision tel que défini à l'article 7, paragraphes (1) et (2), de la loi modifiée du 6 mai 1974 instituant des comités mixtes dans les entreprises du secteur privé et organisant la représentation des salariés dans les sociétés anonymes.

Le consentement de la personne concernée ne rend pas légitime le traitement mis en œuvre par l'employeur.

(2) Sans préjudice du droit à l'information de la personne concernée 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.

(3) Quiconque effectue un traitement en violation des dispositions du présent article est puni d'une peine d'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 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.

(2) Pour les traitements des données dont la mise en œuvre n'est pas susceptible de porter atteinte aux libertés et droits fondamentaux, et notamment à la vie privée, des personnes concernées, la Commission nationale établit et publie des directives en vue d'une notification simplifiée.

Ces directives précisent:

a) la ou les finalités du traitement faisant l'objet d'une notification simplifiée;

b) la ou les catégories de données traitées;

c) la ou les catégories de personnes concernées;

d) les destinataires ou catégories de destinataires auxquels les données sont communiquées;

e) la durée de conservation.

Les traitements qui correspondent à ces directives font l'objet d'une notification simplifiée de conformité envoyée à la Commission nationale le cas échéant par voie électronique.

(3) Est exempté de l'obligation de notification:

(a) le responsable du traitement qui désigne un chargé de la protection des données tenu notamment d'assurer, de manière indépendante, l'application des dispositions légales en la matière et d'établir et de continuer à la Commission nationale un registre des traitements effectués par le responsable du traitement conformément aux dispositions relatives à la publicité des traitements telles que prévues à l'article 15;

(b) le traitement ayant pour seul objet 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) le traitement mis en œuvre conformément aux règles de procédures judiciaires en matière civile et nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice.

(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:

(a) le nom et l'adresse du responsable du traitement, et le cas échéant de son représentant et du sous-traitant;

(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;

(h) la durée de conservation des données.

(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.

(3) La notification se fait auprès de la Commission nationale moyennant support papier ou informatique suivant un schéma à établir par elle. Il est accusé réception de la notification.

(4) Un règlement grand-ducal fixera le montant et les modalités de paiement d'une redevance à percevoir lors de toute notification et de toute modification de notification.

Art. 14. Autorisation préalable de la Commission nationale

(1) Sont soumis à l'autorisation préalable de la Commission nationale:

(a) les traitements prévus à l'article 6, paragraphe (2) lettres (a), (b), (e), (g), et paragraphe (4) lettre (b), à l'article 7, paragraphe (1), et aux articles 10 et 11 de la présente loi;

(b) les traitements de données à des fins historiques, statistiques ou scientifiques visés à l'article 4, paragraphe (2). La Commission nationale vérifie en particulier si ces traitements ne peuvent être réalisés sur base de données rendues anonymes;

(c) l'interconnexion de données visée à l'article 16;

(d) le traitement concernant le crédit et la solvabilité des personnes concernées;

(e) 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.

(2) La demande d'autorisation comprend les informations suivantes:

(a) le nom et l'adresse du responsable du traitement ou de son représentant et le cas échéant du sous-traitant;

(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 aux articles 22 et 23;

(j) la durée de conservation des données.

(3) 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.

(4) 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

(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 (3) (a).

(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,

(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 de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi,

(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

(1) L'interconnexion de données qui n'est pas expressément prévue par un texte légal doit faire l'objet d'une autorisation préalable de la Commission nationale sur demande conjointe présentée par les responsables des traitements en cause.

(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.

(3) L'interconnexion n'est autorisée que dans le respect des finalités identiques ou liées de fichiers et 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).

(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 ci-dessus. 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

(f) le transfert intervienne depuis un registre public tel que prévu à l'article 12,paragraphe (3) lettre (b).

(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 notifier à la Commission nationale un rapport établissant les conditions dans 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

(1) La Commission nationale informe le ministre de toute décision prise en application de l'article 18, paragraphes (3) et (4), et de l'article 19, paragraphes (1) et (2). Le ministre en informe la Commission européenne.

(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

(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. Ces mesures font l'objet d'un rapport annuel à soumettre par le responsable du traitement 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.

(4) Le responsable du traitement agissant dans le cadre de l'accomplissement de ses missions visées à l'article 7, paragraphe (1), 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;
- la durée de conservation 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;
- la durée de conservation 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;

(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 de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi;

(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.

(2) Les dispositions de l'article 26 sont susceptibles de dérogations lors de la collecte de données dans les conditions prévues à l'article 9, paragraphe (1) lettre (c).

(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.

(4) Toute personne a un droit d'accès aux données la concernant et utilisées aux fins d'un traitement mis en œuvre dans le cadre de la liberté d'expression tel que prévu à l'article 9. Aussi longtemps que les données auxquelles l'accès est demandé n'ont pas été publiées, la communication de ces données, ainsi que toute information disponible sur leur origine ne peut se faire que par l'intermédiaire de la Commission nationale.

(5) 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.

(6) 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.

(7) Toute rectification, tout effacement ou verrouillage effectué conformément au paragraphe (5) 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.

(8) Sans préjudice de la sanction prévue au paragraphe (5), 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;

(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 de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi;

(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 et que la mesure d'exception est prise conformément à l'article 28, paragraphe (4);

(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).

(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.

(3) 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.

(4) 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.

(5) Quiconque contrevient à la disposition du paragraphe (3) 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;

(b) de s'opposer, sur demande et gratuitement, au traitement la concernant envisagé par le responsable du traitement 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.

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

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

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

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

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

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

(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.

En cas de cessation du mandat, il est réintégré sur sa demande dans son administration d'origine à un emploi correspondant au traitement qu'il a touché précédemment, augmenté des échelons et majorations de l'indice se rapportant aux années de service passées comme président ou membre effectif jusqu'à concurrence du dernier échelon du grade.

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

(1) Le cadre du personnel de la Commission nationale comprend les fonctions et emplois suivants:

Dans la carrière moyenne de l'administration, grade de computation de la bonification d'ancienneté : grade 7, carrière du rédacteur :

- des inspecteurs principaux 1er en rang
- des inspecteurs principaux
- des inspecteurs
- des chefs de bureau
- des chefs de bureau adjoints
- des rédacteurs principaux
- des rédacteurs

Les agents de la carrière moyenne des rédacteurs sont des fonctionnaires de l'Etat en ce qui concerne notamment leur statut, leur traitement et leur régime de pension qui est régi par les dispositions légales régissant les 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.

(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 à l'article 13 de la présente loi. Pour le solde des frais restant à couvrir dans le cadre de ses missions conférées par la présente loi, la Commission nationale bénéficiera d'une dotation d'un montant à déterminer sur une base annuelle et à inscrire au budget de l'Etat.

(5) La loi du 27 novembre 2001 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2002 est modifiée comme suit:

il est ajouté au budget des dépenses au Chapitre III – Dépenses courantes sous "00 – Ministère d'Etat" une section "00.9 Commission nationale pour la protection des données" émargeant les articles suivants:

"12.300:	Prise en charge par l'Etat des frais encourus par la Commission nationale pour la protection des données. (crédit non limitatif et sans distinction d'exercice)	200.870
33.000:	Dotation initiale en faveur de la Commission nationale pour la protection des données ..	200.000 "

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

(1) Tout responsable de traitement peut, dans le cadre de l'article 12, paragraphe (3) sous (a), et aux fins y visées, 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.

(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:

(a) il ne connaît aucun lien de subordination vis-à-vis du responsable du traitement et ne peut être lié au responsable du traitement par un contrat de travail;

(b) il ne peut être révoqué pour des raisons liées à l'exercice de ses missions, hormis le cas de la violation de ses obligations légales ou conventionnelles.

(4) Le chargé de la protection 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.

(5) 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.

(6) 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 ainsi que d'assises financières d'une valeur de 20.000 euros.

(7) 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.

(8) La Commission nationale vérifie les qualités de tout chargé de la protection des données. Elle peut s'opposer à tout moment à la désignation ou au maintien du chargé de la protection des données lorsqu'il:

(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.

(9) La Commission nationale définit les modalités du contrôle continu des qualités requises à la fonction de chargé de la protection des données.

(10) 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 (ci-après "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.

La centrale des secours d'urgence 112 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.

(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 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.

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).

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.

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.

Le Ministre délégué aux Communications,
François Biltgen

Le Ministre de la Justice,
Luc Frieden

Le Ministre de la Fonction publique
et de la Réforme administrative,
Lydie Polfer

Cabasson, le 2 août 2002.
Henri

Doc. parl. 4735; sess. ord. 2000-2001 et 2001-2002; Dir. 95/46/CE.

Editeur: Service Central de Législation, 43, boulevard F.-D. Roosevelt, L-2450 Luxembourg
Imprimeur: Imprimerie de la Cour Victor Buck, s. à r. l. Leudelange