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:

*

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

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.