

N° 4735<sup>13</sup>

## CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

---

---

**PROJET DE LOI**relatif à la protection des personnes à l'égard du  
traitement des données à caractère personnel

\* \* \*

**RAPPORT DE LA COMMISSION DES MEDIA ET DES COMMUNICATIONS**

(10.7.2002)

La Commission se compose de: M. Laurent MOSAR, Président; M. Patrick SANTER, Rapporteur; Mme Simone BEISSEL, M. Alex BODRY, Mme Mady DELVAUX-STEHRÉS, MM. Robert GARCIA, Marcel GLESENER, Fernand GREISEN, Jean-Marie HALSDORF, Paul HELMINGER et Jean-Paul RIPPINGER, Membres.

\*

**TABLE DES MATIERES**

## Prolégomènes

- A. Antécédents procéduraux
- B. Un équilibre entre société de l'information et protection de la vie privée
- C. Les concepts clés
- I. Le champ d'application
  - A. Le champ d'application matériel et personnel
  - B. Le champ d'application territorial
- II. Les conditions du traitement
  - A. Le principe de la finalité du traitement
  - B. Conditions spécifiques à certains traitements
- III. Les droits de la personne concernée
  - A. Le droit à l'information
  - B. Le droit d'accès
  - C. Le droit d'opposition
  - D. Les décisions individuelles automatisées
- IV. Les formalités de mise en œuvre du traitement
  - A. Le principe: la notification préalable du traitement
  - B. L'exception: l'autorisation préalable du traitement
  - C. Le registre public
- V. Le contrôle du traitement
  - A. Le contrôle externe: la Commission nationale pour la protection des données
  - B. Le contrôle interne
- VI. Les recours juridictionnels
  - A. Les recours de droit commun
  - B. L'action en cessation

- VII. Le transfert de données vers un pays tiers
  - A. Principes
  - B. Exceptions
- VIII. Les dispositions pénales
- IX. Une disposition spécifique et exceptionnelle: l'article 41
- X. Dispositions transitoires et finales; entrée en vigueur
- Conclusion

\*

## PROLEGOMENES

### A. Antécédents procéduraux

Le projet de loi 4735 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel transpose en droit luxembourgeois la directive 95/46/CE du Parlement Européen et du Conseil du 24 octobre 1995<sup>1</sup> (ci-après la „directive“).

Il ne s'agissait pas de la première tentative de transposition de la directive dans notre droit. Dans un premier temps, le gouvernement entendait procéder à une transposition, certes partielle, de la directive afin de remplacer le plus rapidement possible la loi modifiée du 31 mars 1979 déjà obsolète à l'époque<sup>2</sup>.

Le gouvernement ayant décidé de déposer un projet de loi portant transposition intégrale de la directive, le présent projet 4735, le projet de transposition partielle 4357 a été retiré du rôle en mai 1998.

Le projet de loi sous rubrique a été déposé par Monsieur le Ministre délégué aux Communications le 7 décembre 2000. Les chambres professionnelles et autorités suivantes ont émis leurs avis:

- la Chambre des fonctionnaires et employés publics le 22 mai 2001,
- Monsieur le Procureur général d'Etat le 5 juillet 2001,
- la Chambre des employés privés le 30 octobre 2001,
- la Chambre de travail le 14 novembre 2001,
- la Chambre des métiers le 22 novembre 2001, et
- la Chambre de commerce le 13 février 2002.

L'avis du Conseil d'Etat est intervenu le 29 janvier 2002 et a été, ensemble avec le projet de loi et les avis précités, minutieusement examiné par la Commission des médias et des communications (ci-après la „commission“) dans ses réunions du 9 mars 2002 lors de laquelle Monsieur Patrick Santer a été désigné rapporteur, et des 20 mars, 21 mars, 11 avril, 2 mai, 10 mai, 13 mai, 16 mai et 30 mai 2002.

Le 28 mai 2002, la commission a eu une entrevue avec Monsieur le Procureur d'Etat Robert Biever et avec Monsieur le Premier Avocat Général Georges Wivenes. Le 5 juin 2002, elle a adopté des amendements qui ont été avisés par le Conseil d'Etat dans son avis complémentaire du 2 juillet 2002. Cet avis complémentaire a été discuté par la commission lors de sa réunion du 4 juillet 2002. Le 4 juillet 2002, la commission a présenté des amendements au Conseil d'Etat qui furent avisés par celui-ci dans son deuxième avis complémentaire du 9 juillet 2002. Le 10 juillet 2002, la commission a adopté à l'unanimité le présent rapport.

L'article 11 du projet de loi régissant la surveillance sur le lieu de travail a été avisé par la commission du Travail et de l'Emploi. Son avis du 15 mai 2002 est reproduit au document parlementaire 4735<sup>7</sup>.

Les Etats membres auraient dû transposer jusqu'au 24 octobre 1998 la directive en droit luxembourgeois<sup>3</sup>.

N'ayant pas transposé la directive dans ce délai, le Luxembourg a été condamné par la Cour de Justice des Communautés Européennes par arrêt du 4 octobre 2001<sup>4</sup>.

<sup>1</sup> Pour le texte de la directive: doc. parl. 4735, p. 53

<sup>2</sup> Projet de loi 4357

<sup>3</sup> Directive, article 32

<sup>4</sup> Aff C-450/00

Pour être complet, il convient de signaler que la directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications doit encore être transposée en droit luxembourgeois<sup>1</sup>.

Un recours vient d'être introduit contre le Luxembourg pour non-transposition en date du 4 juin 2002<sup>2</sup>.

## B. Un équilibre entre société de l'information et protection de la vie privée

Quiconque lit aujourd'hui la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques<sup>3</sup>, ne peut que constater son obsolescence au regard de l'évolution technologique qui se poursuit depuis quelques années déjà. Cette loi soumet à autorisation ministérielle préalable, après avis préalable d'une commission consultative, la création et l'exploitation de toute banque de données nominatives ne relevant pas de l'Etat. Le caractère illusoire de l'application quotidienne de cette loi ne fait pas de doute.

Adaptée à son époque, elle a été dépassée en raison de l'omniprésence de l'informatique dans notre vie tant professionnelle que privée. Alors qu'à la fin des années 1970, les systèmes informatiques étaient encombrants, peu flexibles et chers, l'apparition des ordinateurs personnels de plus en plus performants<sup>4</sup>, leur démocratisation et l'explosion des services multimédia ont fait de l'ordinateur un outil indispensable à la vie quotidienne. A tel point d'ailleurs que d'aucuns ont relevé l'existence d'une „fracture informatique“ entre ceux qui savent manier un ordinateur et ceux qui ne le savent pas. „Ainsi on est passé d'une société dans laquelle l'informatique était un outil au service des activités humaines à une société de l'information entraînant des modifications structurelles de nos modes de vie.“<sup>5</sup>

L'omniprésence de l'informatique pour bénéfique qu'elle soit recèle des dangers souvent ignorés pour ce qui est de la protection des données à caractère personnel. La personne sujet de l'information – la personne concernée – peut-elle garder la maîtrise sur ce qu'advient de son „double informationnel“? Celui-ci ne risque-t-il pas d'être faussé ou utilisé à des fins non voulues? „L'individu est, en effet, traqué de nos jours dans ses secrets les plus intimes par l'indiscrétion totale croissante tenant à des raisons diverses: contrôles administratifs, intérêts commerciaux, motifs de recherche.“<sup>6</sup> Ces dangers vont croître avec le développement du commerce électronique. „De fait, le commerce électronique favorise la collecte de données personnelles, notamment sur les visiteurs de sites constitués par les entreprises, ou sur les clients. Les visiteurs et les clients sont d'ailleurs, souvent, sollicités lorsqu'ils reviennent sur un site, au moyen des „cookies“ qui ont été implantés sur le disque dur de leur ordinateur lors de leur précédent passage. Les préoccupations pour la protection des personnes que suscitent ces pratiques, et d'autres encore, ont été débattues lors du sommet organisé par l'OCDE à Ottawa en 1998, et l'une des résolutions adoptées à cette occasion est „relative à la protection de la vie privée sur les réseaux mondiaux“ (V. Rev. dr. informatiq. et télécoms, 1998-3, pp. 1001 s.).“<sup>7</sup> La directive et la directive 97/66/CE, dont la transposition ne saurait tarder, trouveront une solution à cette préoccupation.

Dans la mesure où „le partage et la communication internationale de données sont devenus la règle et non l'exception“<sup>8</sup>, deux tendances s'opposent. La première est de dire qu'il s'agit là du prix à payer, d'un sacrifice à supporter si l'on veut profiter des avantages procurés par l'informatique. La seconde est de trouver un équilibre entre la libre circulation des données à caractère personnel et la protection des libertés et droit fondamentaux de la personne concernée.

1 JOCE L24 du 30 janvier 1998

2 affaire C-211/02

3 Modifiée par les lois des 19 novembre 1987, 30 septembre 1992, 1er octobre 1992 et 9 août 1993

4 Plus d'un milliard d'ordinateurs personnels ont été vendus depuis 1971. Le deuxième milliard sera atteint d'ici 2007/2008 (source agence de presse dpa du 2 juillet 2002)

5 Doc. parl. 4735, p. 80

6 Commission nationale Informatique et Libertés (CNIL) (France), Dix ans d'informatique et libertés, Economica, 1988, p. 15

7 Huet, Etude relative aux contrats encadrant les transferts de données personnelles entre les parties à la Convention 108 et les pays tiers n'offrant pas un niveau de protection adéquat, 7-9 février 2001, [www.legal.coe.int](http://www.legal.coe.int).

8 Havelange, Lacoste, Les flux transfrontaliers de données à caractère personnel en droit européen, JTDE 2001, p. 241

En effet, le respect de ces droits et libertés, parmi lesquels le droit à la vie privée, constitue un fondement de notre Etat de droit. L'article 8 de la Charte des droits fondamentaux de l'Union Européenne annexée au traité de Nice<sup>1</sup> reconnaît expressément le droit à la protection des données à caractère personnel. Celui-ci doit également être rangé parmi les „droits naturels et la personne humaine et de la famille“ dont l'Etat doit garantir le respect en vertu de l'article 11 (3) de la Constitution ou – pour reprendre la formulation proposée par la Chambre des Députés dans le cadre de la révision de l'article 11 – parmi les „droits fondamentaux de la personne humaine“<sup>2</sup>.

C'est cette seconde voie, à savoir celle de la conciliation entre les deux objectifs, qui a été, à juste titre, choisie par la directive, comme le démontre son intitulé, puisqu'elle est „relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données“.

La directive reprend l'option choisie en son temps par la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, entrée en vigueur le 1er octobre 1985<sup>3</sup>.

La directive part du constat que les flux transfrontaliers de données à caractère personnel vont augmenter avec la continuation de l'intégration économique et le fonctionnement du marché intérieur ainsi qu'avec le renforcement de la coopération scientifique et technique et la mise en place de nouveaux réseaux de télécommunications dans la Communauté Européenne. Cependant, elle relève que les disparités dans les dispositions nationales quant au niveau de protection des droits et libertés des personnes à l'égard de traitement de données à caractère personnel „peuvent empêcher la transmission de ces données du territoire d'un Etat membre à celui d'un autre Etat membre; que ces différences peuvent dès lors constituer un obstacle à l'exercice d'une série d'activités à l'échelle communautaire, fausser la concurrence et empêcher les administrations de s'acquitter des responsabilités qui leur incombent en vertu du droit communautaire“<sup>4</sup>.

Une coordination au niveau communautaire des législations nationales s'imposait. La directive vise à concilier la libre circulation des données au sein de l'Union Européenne et la protection des droits et libertés des personnes concernées. La directive tend à l'établissement d'un „niveau élevé de protection dans la Communauté“<sup>5</sup>. Cet équilibre, certes délicat, se retrouve dans le projet de loi 4735.

Loin de les rendre superflus, „les principes de la protection des droits et libertés des personnes, notamment du droit à la vie privée, contenus dans la (...) directive précisent et amplifient ceux qui sont contenus“ dans la Convention 108 du Conseil de l'Europe<sup>6</sup>.

### C. Les concepts clés

La compréhension de la portée du projet de loi 4735 suppose la connaissance d'un certain nombre de concepts clés qui reviendront tout au long du texte du projet de loi.

#### *1) Le consentement de la personne concernée (article 2, lettre (c))*

Il s'agit d'une notion essentielle de la loi à venir. Ainsi, par exemple, un tel consentement permet de légitimer un traitement<sup>7</sup> ou de transférer des données n'assurant pas un niveau de protection adéquat<sup>8</sup>. Ce principe n'est cependant pas général<sup>9</sup>.

Le consentement de la personne au traitement de ses données doit être exprès et non équivoque. Aucune forme écrite et aucune formule sacramentelle ne sont requises.

1 JOCE du 18 décembre 2000 C-364/10

2 Doc. parl. 3923 B-2

3 Cette convention a été ratifiée par 28 Etats membres du Conseil de l'Europe (situation au 12 juin 2002, source: www.coe.int). Le Luxembourg a ratifié la Convention 108 le 10 février 1988. A noter qu'un protocole additionnel à la Convention 108 a été ouvert à la signature le 8 novembre 2001. Au 12 juin 2002, le Luxembourg n'a pas encore signé ce protocole additionnel.

4 Directive, considérant 7

5 Directive, considérant 10

6 Directive, considérant 11

7 Art. 5 (1) lettre (f)

8 Art. 19 (1) lettre (a)

9 Voir art. 6, paragraphe (1) lettre (a), 6, paragraphe (4) lettre (b), 11 paragraphe (1)

Le consentement doit être libre. Les auteurs du projet de loi ont cru pertinent de procéder à une appréciation critique de la liberté du consentement. Ils soulignent qu'en présence d'une situation dans laquelle le responsable du traitement se trouve en position de force face à la personne concernée, comme par exemple lorsque la personne concernée souhaite obtenir un prêt bancaire ou souscrire une assurance-vie, il peut „s'avérer fort probable que le consentement de la personne concernée n'est pas forcément libre“<sup>1</sup>.

La liberté du consentement doit s'apprécier au cas par cas au regard des circonstances de l'espèce. Pour ce faire, les articles 1112 et suivants du Code civil tels qu'appliqués par la jurisprudence<sup>2</sup> serviront de lignes directrices en la matière.

Le consentement doit être spécifique, en ce qu'il ne peut porter que sur des traitements déterminés. C'est dans cette optique que le responsable du traitement doit informer la personne concernée sur la ou les finalités déterminées du traitement auquel les données sont destinées<sup>3</sup>. Si plusieurs finalités sont poursuivies par un même traitement, le responsable du traitement doit en informer la personne concernée<sup>4</sup>.

Finalement le consentement doit être informé. La personne concernée doit donner son consentement en connaissance de cause, ce qui explique une nouvelle fois le lien entre le consentement de la personne concernée avec le principe de la qualité des données prévu à l'article 4, paragraphe (1) lettre (a), et avec le droit à l'information prévu à l'article 26. Ce droit à l'information doit s'exercer soit lors de la collecte des données auprès de la personne concernée, soit lors de l'enregistrement ou la première communication à un tiers pour les données qui n'ont pas été collectées auprès de la personne concernée.

### 2) La donnée à caractère personnel – la donnée (article 2, lettre (e))

Il y a donnée lorsqu'une information quels que soient sa nature ou son support concerne une personne identifiée ou identifiable. „Une personne est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique“<sup>5</sup>, comme par exemple le numéro de passeport, un numéro de téléphone ou celui d'une plaque minéralogique.

Une donnée codée tombe dans la définition précitée, dès lors que la personne concernée peut être identifiée ou identifiable<sup>6</sup>. L'identification peut se faire par „toute forme de captage, de traitement et de diffusion de sons ou d'images“<sup>7</sup>.

Une donnée anonyme en est au contraire exclue. Une donnée rendue anonyme également, mais uniquement à partir du moment où elle a été rendue anonyme, à condition qu'on ne puisse plus procéder à l'identification de la personne concernée.

Pour être réputée anonyme ou rendue anonyme, il faut qu'il s'agisse d'une donnée pour laquelle il n'existe aucun moyen technique, soit dans le chef du responsable du traitement, soit même dans le chef d'un tiers, permettant de rattacher cette donnée à un individu<sup>8</sup>. Il appartient au responsable du traitement d'apporter la preuve que les données qu'il traite sont à qualifier de données anonymes<sup>9</sup>.

### 3) Le fichier (article 2, lettre (h))

Un tel fichier doit être structuré pour que le projet de loi trouve à s'appliquer. Le projet de loi ne s'applique donc pas à n'importe quel fichier. Peu importe la structure appliquée à un tel fichier. Il s'agit de la définition utilisée à l'article 2 c) de la directive<sup>10</sup>.

1 Doc. parl. 4735, p. 27

2 Voir p.ex. Cour 6 octobre 1993, Pas. 29, 279

3 Voir article 26

4 Sur les finalités induites: voir II. A. 1) a

5 Article 2 lettre (e)

6 Leonard, Poulet, La protection des données à caractère personnel en pleine (r)évolution, JT 1999, p. 377, part. p. 378, note (16)

7 Article 3, paragraphe (4)

8 Directive, considérant 26

9 Doc. parl. 4735, p. 25

10 Voir aussi article 3, paragraphe (1)

4) *L'instance médicale (article 2, lettre (i))*

Dans son avis complémentaire du 2 juillet 2002, le Conseil d'Etat a émis des doutes sur les conséquences de l'inclusion de la loi du 28 août 1998 sur les établissements hospitaliers à l'endroit de l'article 2, lettre (i). La commission maintient la définition de l'instance médicale, alors que celle-ci a précisément été confortée par les instances gouvernementales compétentes.

5) *Le responsable du traitement (article 2, lettre (o))*

Le responsable du traitement dispose du pouvoir décisionnel pour déterminer les finalités poursuivies par un traitement et les moyens à mettre en œuvre en vue de ce traitement. Il se distingue ainsi du sous-traitant<sup>1</sup> chargé de l'exécution matérielle de tout ou partie du traitement.

Un même traitement peut être soumis conjointement à plusieurs responsables d'un traitement. Si, par exemple, plusieurs sociétés d'assurance ou de réassurance décident de s'associer pour couvrir une catégorie particulière de risques sans créer pour ce faire une entité juridique distincte, elles seront chacune considérées comme responsable du traitement pour les données traitées dans le cadre de cette association.

6) *Le traitement (article 2, lettre (s))*

Le traitement remplace la notion de „banque de données“ utilisée par la loi du 31 mars 1979. C'est en effet non la création d'une „banque de données“, comprise comme lieu où les données sont conservées, mais le traitement de ces données qui peut donner lieu à des abus. La focalisation s'est déplacée du lieu de stockage des données au traitement de celles-ci.

\*

***Deux remarques pour terminer cette introduction:***

D'une part, le langage courant désigne cette matière sous le terme générique de „protection des données“. Or le présent projet de loi n'a pas pour objet de protéger les données. Il faut au contraire protéger les personnes dont les données qui font l'objet d'un traitement contre tout abus en la matière pour assurer le respect de leurs droits et libertés fondamentales.

D'autre part, il a été reproché au projet de loi sous rubrique d'être un „fourre-tout“ de dispositions et qu'il aurait été plus approprié de suivre une approche „sectorielle“ au lieu d'édicter un texte à vocation horizontale. La commission approuve l'option du gouvernement, dans la mesure où tout un chacun retrouve dans un seul et même texte l'ensemble des dispositions concernant le traitement des données<sup>2</sup>.

\*

## **I. LE CHAMP D'APPLICATION**

### **A. Le champ d'application matériel et personnel**

Tout en transposant la directive en droit luxembourgeois, le projet de loi va parfois au-delà de ce qui est exigé dans le texte communautaire.

Ainsi le champ d'application de la directive a-t-elle été élargi par le projet de loi aux intérêts légalement protégés des personnes morales<sup>3</sup>. Les intérêts légalement protégés des personnes morales constituent le pendant des libertés et droits fondamentaux de la personne physique.

Il serait faux de croire que le bénéfice de la protection assurée par le biais du présent projet de loi soit dépendant de l'existence de la personnalité juridique. Ainsi les groupements de fait, dépourvus d'une telle personnalité juridique, doivent être comptés parmi les personnes concernées<sup>4</sup>.

Le champ d'application personnel est donc suffisamment vaste.

1 Défini à l'article 2, lettre (p)

2 Par la suite, nous utiliserons les termes tels que définis à l'article 2 de la directive

3 Article 1er. La législation belge continue d'exclure les personnes morales de son champ d'application: Léonard et Poulet, op. cit., JT 1999, p. 380

4 Article 2, lettre (n)

En ce qui concerne le champ d'application matériel, la défense, la sécurité publique, la sûreté de l'Etat et les activités de l'Etat dans le domaine pénal, qui ne sont abordées par la directive qu'à titre facultatif, sont intégrées dans le champ d'application du projet de loi, comme cela avait d'ailleurs déjà été le cas pour la loi du 31 mars 1979<sup>1</sup>. La loi de 1979 se trouve cependant précisée sur ce point, comme nous le verrons par après.

Toujours en ce qui concerne le champ d'application *ratione materiae*, l'article 3, paragraphe (1), ainsi que l'article 2, lettre (s), précisent que le traitement n'a pas besoin d'être entièrement automatisé. „Si au moins une des opérations, dont l'ensemble constitue le traitement tel que défini à l'article 2 du présent projet, est effectuée de façon automatisée, les autres l'étant de façon „manuelle“, le traitement doit être opéré en conformité avec les dispositions de la présente loi<sup>2</sup>.“ Ainsi, par exemple, si les données sont collectées par un sondeur lors d'un entretien avec la personne concernée sur base d'un formulaire avec des cases à cocher, mais que leur enregistrement est effectué de manière automatisée, les dispositions du projet de loi s'appliquent.

A cela s'ajoute que même en présence d'un traitement non automatisé le projet de loi retrouve application, dès lors que les données ainsi traitées figurent ou sont appelées à figurer dans un fichier. Un tel fichier doit être structuré „selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause“<sup>3</sup>. Ainsi, un fichier manuel peut être considéré comme structuré au sens du projet de loi et de la directive, si, par exemple, il range les noms des personnes concernées par ordre alphabétique. Comme indiqué précédemment ce n'est que le fichier absolument dénué de toute structuration qui échappe au projet de loi.

L'article 3, paragraphe (5), exclut deux catégories de traitement de son champ d'application.

Il s'agit, d'une part, d'écarter, au nom du respect dû à la vie privée, du champ d'application du projet de loi les traitements mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, par exemple, la correspondance ou la tenue d'un répertoire d'adresses<sup>4</sup>. Dès que le traitement ne vise plus exclusivement les activités personnelles ou domestiques d'une personne physique et est utilisé, ne serait-ce que partiellement pour une activité professionnelle ou sort, ne serait-ce que provisoirement, de la sphère privée de cette personne, les dispositions du projet s'appliquent.

D'autre part, ne sont également pas couverts par le projet de loi les traitements concernant une personne morale dont la publication est requise par la loi ou un règlement. Sont plus particulièrement visées les données des personnes morales qui doivent être publiées au Mémorial en application de la loi modifiée du 10 août 1915 sur les sociétés commerciales.

## B. Le champ d'application territorial<sup>5</sup>

Le champ d'application *ratione loci* est déterminé par l'article 3, paragraphe (2) du projet de loi. Cette disposition est particulièrement importante au regard de la libre circulation des données au sein de l'Union européenne. Elle vise à éviter à la fois les situations où aucune législation sur la protection des données ne s'applique et les situations dans lesquelles deux ou plusieurs législations nationales viendraient à s'appliquer cumulativement.

### 1. Le responsable du traitement soumis au droit luxembourgeois (article 3, paragraphe (1) lettre (a))

Le projet de loi s'applique au traitement effectué par un responsable du traitement soumis au droit luxembourgeois. Est soumis au droit luxembourgeois le responsable du traitement qui est établi au Luxembourg. L'article 3, paragraphe (1) lettre (a), reprend les dispositions de l'article 3, paragraphe (1),

1 Voir article 12 de la loi de 1979

2 Doc. parl. 4735, p.28

3 Directive, considérants 15 et 27

4 Directive, considérant 12

5 Pour la détermination du champ d'application de la directive à des sites Internet localisés en dehors de l'Union Européenne: voir rapport du groupe institué à l'article 29 de la directive adopté le 30 mai 2002 („Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU web sites 5035/01/EN/Final WP56, [www.europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/index.htm](http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm))

lettre (a) et lettre (b), premier tiret, du texte soumis par la commission au Conseil d'Etat le 5 juin 2002. Le second tiret du paragraphe (3) lettre (b) devient le paragraphe (3) lettre (b) à lui tout seul.

La version initiale du projet de loi, plus proche de l'article 4 de la directive, exigeait que le responsable du traitement soit „établi sur le territoire luxembourgeois ou en un lieu où, selon le droit international public, est applicable le droit luxembourgeois“. Le texte adopté par la commission qui, plus concis, se contente de prévoir que le responsable du traitement doit être soumis au droit luxembourgeois, c'est-à-dire établi sur le territoire luxembourgeois sans référence au droit international public. Cette différence avec le texte initial ne prête à aucune conséquence.

Partant, sont concernés les traitements effectués „dans le cadre des activités d'un établissement du responsable“ sur le territoire luxembourgeois<sup>1</sup>. La forme juridique de cet établissement, succursale ou filiale, importe peu. L'établissement exige cependant „l'exercice effectif et réel au moyen d'une installation stable“<sup>2</sup>. C'est dans le cadre de l'exercice des activités de cet établissement situé au Luxembourg que le traitement doit être effectué pour que les dispositions de la loi à venir puissent trouver à s'appliquer. On ne tiendra pas compte du lieu d'établissement du sous-traitant.

Si, pour reprendre l'exemple avancé par le Professeur Braibant et repris dans l'exposé des motifs<sup>3</sup>, une entreprise française fabrique au Portugal des marchandises qu'elle vend à partir d'un établissement situé en France à des clients allemands, les traitements de données concernant le site de production seront soumis au droit portugais et les traitements se rattachant à la gestion de la clientèle allemande seront régis par le droit français, car les ventes sont le fait d'un établissement français.

Ce critère de l'établissement est clair et a le mérite d'empêcher des situations dans lesquelles un traitement pourrait être soumis à une multitude de législations applicables.

Si, par exemple, un établissement français se voit confier la gestion de données relatives à la gestion du personnel ou du stock d'établissements anglais, allemands, portugais et luxembourgeois, on évite l'application cumulative des lois française, anglaise, allemande, portugaise et luxembourgeoise à un seul traitement. En effet alors même que ce traitement unique de données „multinationales“ est effectué au bénéfice de tous les établissements précités, il n'est mis en œuvre que dans le cadre des activités de l'établissement français. Il ne faut donc pas analyser qui est le bénéficiaire du traitement, mais déterminer dans le cadre des activités de quel établissement le traitement est réalisé. Dans l'exemple précité, le traitement est effectué par l'établissement français dans le cadre de ses activités. „Les autres sociétés, au profit desquelles le traitement est poursuivi, ne seraient soumises qu'à leurs lois dans la mesure où elles effectuent un nouveau traitement à l'aide des données centralisées“<sup>4</sup>. Dans pareille situation, les autres sociétés prendraient chacune la qualité de responsable du traitement pour les traitements ultérieurs.

L'OCDE considère qu'un site web n'est pas un établissement stable. Un accord sur l'hébergement d'un tel site n'aboutit pas à créer un établissement stable pour l'entreprise qui exerce ses activités par le biais de ce site. L'établissement du fournisseur de services n'est pas, en principe, à prendre en considération. Un local qui héberge des équipements informatiques peut constituer un établissement si des activités sont exercées par l'intermédiaire de ce local<sup>5</sup>.

Sont aussi visés les traitements effectués par un responsable du traitement établi en un lieu où, conformément aux règles du droit international public, est applicable le droit luxembourgeois.

## *2. Les moyens de traitement établis sur le territoire luxembourgeois (article 3, paragraphe (1) lettre (b))*

Ce n'est pas parce que le responsable du traitement n'est pas établi sur le territoire luxembourgeois ou en un lieu où le droit luxembourgeois est applicable, que le projet de loi n'a pas vocation à s'appliquer.

Si le responsable du traitement n'est pas établi au Luxembourg ni dans un autre Etat membre de l'Union européenne, la loi luxembourgeoise s'applique à ce traitement si ce responsable utilise des

1 Directive, article 4, paragraphe 1, lettre a)

2 Directive, considérant 19

3 Doc. parl. 4735, p. 29

4 Léonard, Pouillet, op. cit., p. 382

5 Verbiest, Wéry, Le droit de l'internet et de la société de l'information, Larcier 2001, pp. 393 et ss., Havelange, Lacoste, op. cit. p. 243

moyens de traitement situés sur le territoire luxembourgeois ou, bien que cela ne figure pas *expressis verbis* dans le texte, en tout autre lieu où s'applique le droit luxembourgeois.

Les moyens de traitement doivent s'entendre de manière large, c'est-à-dire tant des équipements que des moyens en personnel.

Cette disposition, protectrice des droits de la personne concernée<sup>1</sup>, empêche le responsable du traitement d'échapper à l'emprise de la loi à venir en se délocalisant hors de l'Union européenne.

Si uniquement des moyens utilisés à des fins de transit sont situés sur le territoire luxembourgeois ou sur celui d'un autre Etat membre de l'Union européenne, le projet de loi sous rubrique ne s'applique pas à un tel traitement. Cette exception doit être interprétée restrictivement. Aucun traitement, ni aucune partie de celui-ci, ne doivent avoir lieu au Luxembourg ou sur le territoire d'un autre Etat membre au risque de voir appliquée la législation luxembourgeoise ou, le cas échéant, celle de cet autre Etat membre.

Lorsque le projet de loi s'applique et que le responsable du traitement n'est pas établi au Luxembourg, il doit désigner un représentant établi au Luxembourg qui se substitue à lui dans l'accomplissement des obligations imposées à un responsable du traitement établi au Luxembourg.

Il découlait de la proposition de texte faite par le Conseil d'Etat que cette désignation ne devait se faire que dans l'hypothèse de l'utilisation de moyens sur le territoire luxembourgeois à des fins de transit. Cette proposition aurait contrevenu aux dispositions de l'article 4, paragraphe 2., de la directive.

Cette substitution du responsable du traitement par un représentant établi au Luxembourg se fait par déclaration écrite adressée à la Commission nationale. Il va de soi que tout remplacement d'un représentant devra être déclaré à cette autorité.

Le représentant accomplit tous les actes que le responsable du traitement aurait dû accomplir s'il était établi lui-même au Luxembourg<sup>2</sup>. Les relations entre le responsable du traitement et son représentant peuvent être empreintes d'un lien de subordination caractéristique d'un contrat de travail ou, au contraire, d'une certaine autonomie comme dans un mandat. En tout cas, cette substitution ne dégage pas le responsable du traitement de sa propre responsabilité. Toute clause contraire serait nulle et non avenue.

Pour ce qui est de données collectées au Luxembourg<sup>3</sup> et transférées hors de l'Union européenne, nous renvoyons au point VII. ci-après.

\*

## II. LES CONDITIONS DU TRAITEMENT

Le projet de loi prévoit en premier lieu des conditions générales pour effectuer un traitement (A.). Eu égard à certaines catégories particulières de données ou certains traitements spécifiques, des conditions supplémentaires ont été imposées (B.).

### A. Le principe de la finalité du traitement

„Un traitement d'informations nominatives est créé pour atteindre un certain but. Il doit être adapté et ne pas servir à d'autres fins. Ce principe de finalité est omniprésent.“<sup>4</sup> Le principe de la finalité a une portée double: d'un côté les données doivent être traitées loyalement et licitement (article 4) (1.) et le traitement ne peut être effectué que s'il est légitime (article 5) (2.). En d'autres termes, l'article 5 répond à la question de savoir quand un traitement peut être mis en œuvre, l'article 4 à celle de savoir comment effectuer un tel traitement.

Le lien entre les deux dispositions est évident. Ce n'est pas parce que les données sont traitées conformément aux dispositions de l'article 4 que le traitement est automatiquement légitime ou légi-

1 Directive, considérant 20

2 Dans la suite du texte du projet de loi, toute référence au responsable du traitement s'applique mutatis mutandis à son représentant

3 Rappelons que la collecte fait partie intégrante de la notion de traitement

4 CNIL, Dix ans d'informatique et libertés, op. cit., p. 81

timé. Ce n'est pas parce que le traitement est légitime au regard de l'article 5 que, de ce simple fait, le responsable du traitement peut s'affranchir de respecter les règles édictées par l'article 4.

### 1. La qualité des données

Les données doivent être traitées loyalement et licitement. Le responsable du traitement doit s'en assurer, et non plus comme indiqué dans la version initiale, le garantir.

Le traitement loyal et licite implique „notamment“ quatre conséquences, mentionnées à l'article 4, paragraphe (1)<sup>1</sup>. Il s'agit d'une énumération non limitative.

- a. Les données doivent être collectées pour „des finalités déterminées, explicites et légitimes“. Elles ne doivent pas être „traitées ultérieurement de manière incompatible avec ces finalités“.

La finalité doit être déterminée et explicite lors de la collecte<sup>2</sup>. Il s'agit d'un élément indispensable pour que la personne concernée puisse donner son consentement libre, spécifique et informé. La finalité doit être transparente. La personne concernée doit savoir à quoi serviront ses données.

Il est difficile de circonscrire la notion de finalité, ce qui explique l'absence de définition dans la directive et dans le projet de loi. Cependant „il ne peut (...) être question d'englober dans une finalité un ensemble d'objectifs flous et trop nombreux“<sup>3</sup>.

Sous l'empire de la législation belge datant d'avant la transposition de la directive, la jurisprudence avait précisé que „doit faire l'objet d'une transparence chaque traitement, c'est-à-dire tout ensemble d'opérations marquées par une finalité unique telle que la personne concernée puisse raisonnablement, à la lecture de l'énoncé de cette finalité, concevoir les types d'opérations couvertes par cette finalité“<sup>4</sup>.

Il convient cependant de relever que dans bien des cas un seul traitement peut poursuivre plusieurs finalités.

Pour qu'un seul traitement puisse poursuivre plusieurs finalités, les principes dégagés aux articles 4 et 5 du projet de loi doivent rester inchangés. Si l'un ou l'autre des ces principes se trouve modifié au regard d'une seconde finalité que le responsable du traitement entend réaliser, un nouveau traitement, avec toutes les conséquences que cela implique (par exemple: nouvelle notification à, ou autorisation de, la Commission nationale) doit être effectué. Ainsi verrons-nous plus loin que les données doivent être „adéquates, pertinentes et non excessives“ au regard des finalités. Si un responsable du traitement envisage une première finalité nécessitant le traitement d'un certain nombre de données et une seconde finalité qui ne requiert le traitement que de certaines de ces données, il devra effectuer deux traitements différents, car le traitement de toutes les données sera certes proportionné au regard de la première finalité, mais ne le sera plus pour poursuivre la seconde finalité.

C'est aussi le principe de transparence qui explique pourquoi un traitement ultérieur doit être compatible avec la ou les finalités communiquées à la personne concernée lors de la collecte.

L'article 4, paragraphe 1er, de la loi belge du 11 décembre 1998 précise que la compatibilité doit tenir compte „notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables“. La doctrine a critiqué une compatibilité automatique en cas de changement de finalité dû à une modification légale ou réglementaire<sup>5</sup>. Le présent projet de loi ne saurait être interprété comme permettant une telle compatibilité automatique en cas de changement de l'environnement légal ou réglementaire. Cependant il ne saurait être exclu que, dans une situation particulière, un tel changement puisse être considéré comme compatible avec la finalité initiale, sans qu'il y ait automatisme.

Avant tout traitement ultérieur qui ne serait pas compatible avec la finalité déjà communiquée, le responsable du traitement devra en informer la personne concernée et recueillir son consentement, à moins naturellement qu'il puisse justifier le traitement par l'un des autres critères mentionnés à

1 Relevons que la directive fait figurer le traitement loyal et licite comme une des cinq conséquences du principe de la qualité des données, alors que le projet de loi pose le traitement loyal et licite comme principe et en fait découler les 4 conséquences qui sont reprises de la directive. Cette différence ne prête à aucune conséquence.

2 Directive, considérant 28

3 Pipers, *Le respect de la vie privée*, cité in doc. parl. 4735, p. 30

4 Buyle, Lanoye, Pouillet, Willems, *Chronique de jurisprudence „informatique“*, JT 1996, No 65, p. 233

5 Léonard, Pouillet, op. cit., p. 385

l'article 5, paragraphe (1). Afin d'éviter que le responsable du traitement puisse être amené à réduire le droit d'information de la personne concernée à sa portion congrue, la compatibilité d'un traitement ultérieur avec la finalité initiale doit être examinée avec circonspection.

Le projet de loi prévoit un régime à part pour une catégorie déterminée de traitements ultérieurs, à savoir les traitements ultérieurs à des fins historiques, statistiques ou scientifiques. L'article 4, paragraphe (2), précise que des données traitées pour une finalité déterminée peuvent faire l'objet d'un traitement ultérieur, mais uniquement à des fins historiques, statistiques ou scientifiques. Un tel traitement ultérieur doit être préalablement autorisé par la Commission nationale qui vérifiera si ce traitement ne peut être effectué sur base de données rendues anonymes<sup>1</sup>, c'est-à-dire ne permettant plus d'identifier la ou les personnes concernées.

- b. Les données doivent être „adéquates, pertinentes et non excessives au regard des finalités“ de la collecte.

Il s'agit là du principe de proportionnalité. Le responsable du traitement devra, avant de commencer un traitement, s'interroger sur les catégories de données à collecter pour pouvoir atteindre les finalités qu'il s'est fixées. La collecte des données ne doit pas aller au-delà de ce qui est nécessaire au regard de la ou des finalités poursuivies.

Ainsi, par exemple, viole ce principe de proportionnalité une banque qui „ne s'est pas contentée de cibler sa clientèle sur base de données recueillies dans le cadre de la gestion des comptes afin de lui vendre un produit; [qu'] à l'occasion de cette campagne, elle a recherché et collecté de nouvelles données relatives à l'état du portefeuille clients ayant un prêt logement à l'OCCH“, en l'espèce d'un concurrent dont la banque en question s'était portée acquéreur<sup>2</sup>. Le traitement d'informations n'ayant aucun lien avec une finalité déterminée est à considérer comme excessif et contraire au principe de proportionnalité.

- c. Les données doivent être „exactes et, si nécessaire, mises à jour“.

Cette précision s'impose d'elle-même. Elle figure également à l'article 28, paragraphe (5).

Le projet de loi oblige le responsable du traitement de prendre „toute mesure raisonnable“ pour que des données inexacts ou incomplètes au regard des finalités soient effacées ou rectifiées. Cette obligation de diligence s'apprécie en fonction du bon père de famille que doit être le responsable du traitement et en fonction de la finalité poursuivie par le traitement.

- d. Les données doivent être „conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités“ poursuivies.

Dans la mesure où seules les données „adéquates, pertinentes et non excessives“ doivent être traitées, la durée de leur conservation doit également être proportionnée à la réalisation de la finalité poursuivie. Dès que les données ne sont plus nécessaires, elles doivent être effacées, sans préjudice de la possibilité d'un traitement ultérieur à des fins historiques, statistiques ou scientifiques en application des conditions posées à l'article 4, paragraphe (2).

## 2. La légitimité du traitement

Un traitement peut être effectué dans l'une des six hypothèses de l'article 5, paragraphe (1). Cette énumération est limitative. L'illégitimité peut également survenir en cours de traitement dès lors que le traitement ne se situe plus dans le cadre tracé par l'une des ces hypothèses.

- a. „Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis.“

Sont par exemple visées les communications des données concernant le personnel, effectuées par une société aux organismes de sécurité social.

- b. „Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées.“

<sup>1</sup> Article 14, paragraphe (1), lettre (b)

<sup>2</sup> Comm. Bruxelles, 15 septembre 1994, cité in Buyle, Lanoye, Pouillet, Willems, op. cit. No 72, p. 236

Cette disposition concerne le secteur public. La notion de „secteur public“ doit être interprétée de manière extensive en ce que les chambres professionnelles, pour ne citer qu’elles, doivent y être comprises.

Pour que cette disposition s’applique, soit le responsable du traitement soit le tiers auquel les données ont été communiquées doivent relever du secteur public.

L’article 5, paragraphe (1) lettre (b), ne doit pas cacher l’existence d’une autre contrainte s’appliquant en la matière. Il faut en effet respecter les exigences posées à l’article 8, paragraphe 2, de la Convention européenne des droits de l’homme<sup>1</sup> qui prévoit que „il ne peut y avoir ingérence d’une autorité publique dans l’exercice [du droit au respect de la vie privée et familiale] que pour autant que cette ingérence est prévue par la loi et qu’elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité publique, au bien-être économique du pays, à la défense de l’ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d’autrui“.

- c. „Le traitement est nécessaire à l’exécution d’un contrat auquel la personne concernée est partie ou à l’exécution de mesures précontractuelles prises à la demande de celle-ci.“

L’exécution du contrat ou l’exécution réclamée par la personne concernée d’une mesure précontractuelle est dans l’intérêt de la personne concernée, puisque celle-ci a consenti au contrat et à son exécution ou a demandé l’exécution d’une mesure précontractuelle. Ce serait sinon mettre le responsable du traitement dans l’impossibilité d’exécuter sa partie du contrat. Cette légitimité se trouve dans la droite ligne du principe de l’exécution de bonne foi de toute convention figurant à l’article 1134 du Code civil.

En cas de résolution du contrat, les données collectées devront être effacées. En cas de résiliation, le traitement devra immédiatement cesser et l’effacement des données pourra s’imposer au regard des circonstances de l’espèce.

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

La disposition figurant sous la lettre (d) réitère expressis verbis l’exigence d’une balance nécessaire entre, d’un côté, les intérêts légitimes du responsable du traitement ou des tiers qui ont reçu communication des données, et, de l’autre côté, les intérêts et les droits et libertés fondamentaux de la personne concernée.

Cette balance des droits, libertés et intérêts des parties en cause est sous-jacente dans les autres hypothèses visées à l’article 5, paragraphe (1).

La lettre (d) se situe résolument dans le cadre tracé par l’article 1er du projet de loi. Le traitement est illégitime dès lors que la balance penche en défaveur de la personne concernée. Il appartient à la Commission nationale de surveiller le respect de cette balance.

Le document parlementaire 4735 énumère aux pages 31 et 32 quelques exemples illustrant le respect d’une telle balance des intérêts en cause.

Nous voudrions brièvement approfondir le deuxième exemple. Il y est précisé que „les données à caractère personnel sont traitées à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, à condition toutefois que les résultats soient publiés sous une forme ne permettant pas d’identifier les personnes concernées“.

C’est dans le cadre de cet exemple qu’il convient de considérer la situation décrite au considérant 30 de la directive. Ce considérant autorise les Etats membres „en vue d’assurer l’équilibre des intérêts en cause, tout en garantissant une concurrence effective (...) [à] préciser les conditions dans lesquelles des données à caractère personnel peuvent être utilisées et communiquées à des tiers dans le cadre d’activités légitimes de gestion courante des entreprises et autres organismes“.

<sup>1</sup> Cette disposition est d’ordre public (CE 17 juillet 1992, Pas. 28, 288) et d’effet direct, c’est-à-dire qu’elle crée au profit des justiciables des droits que les juridictions nationales sont chargées de sauvegarder (Cour 13 novembre 1996, Pas. 30, 154)

Il semble par trop péremptoire que d'affirmer que les résultats des traitements de données effectués par exemple dans le cadre d'une planification ne devraient jamais permettre d'identifier les personnes concernées lorsque ces résultats sont publiés.

En effet, par exemple en vue de rationaliser une répartition intragroupe des tâches, si la société faitière d'un groupe de sociétés, dont au moins une est établie au Luxembourg, décide de faire le relevé du personnel employé, de la description des postes occupés, du nombre de salariés ainsi que de la rémunération payée et autres avantages consentis à ces salariés, sans que ces données soient publiées ailleurs qu'au sein dudit groupe, on ne saurait douter a priori du caractère légitime d'un tel traitement. Certes des relevés globaux sont envisageables. Mais il peut exister des postes qui, par leur nature ou parce qu'ils ne sont occupés que par une seule personne<sup>1</sup>, permettent l'identification de la personne concernée malgré l'existence de relevés globaux. En pareille circonstance, et sous réserve des circonstances de l'espèce, on peut néanmoins partir du principe de la légitimité d'un tel traitement.

Il doit en aller de même, toujours sous la même réserve que précédemment, lorsqu'une personne souhaite se porter acquéreur d'une société et, avant de signer le contrat d'achat, fait procéder à l'inventaire des actif et passif de cette société. Les données ainsi recueillies doivent pouvoir être traitées.

e. „Le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée.“

f. „La personne concernée a donné son consentement.“

Il est renvoyé à la page 32 du document parlementaire 4735 pour les conséquences du retrait d'un consentement.

## **B. Conditions spécifiques à certains traitements**

### *1. Le traitement des données sensibles*

Le traitement de données sensibles est régi par l'article 6. La structure de cet article, pour complexe qu'elle soit<sup>2</sup>, a été reprise de la directive et est logique. Le premier paragraphe établit le principe de l'interdiction du traitement des données sensibles. Les exceptions sont prévues aux paragraphes (2) à (3). Le paragraphe (4) traite des données génétiques et le paragraphe (5) fixe les sanctions pénales.

Les traitements de données sensibles ne sont pas interdits en tant que tels. C'est uniquement lorsque le traitement de ces données révèle „l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les traitements de données relatives à la santé et à la vie sexuelle“ que ce traitement tombe sous la prohibition du paragraphe (1)<sup>3</sup>. Elargissant le champ d'application de la directive en la matière, le projet de loi ajoute que l'interdiction s'étend au traitement des données génétiques.

La loi belge du 11 décembre 1998 dispose que les données sensibles sont celles qui „révèlent l'origine raciale ou ethnique, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la vie sexuelle“.

Le projet de loi se démarque de la législation belge en ce que l'accent est mis sur le traitement des données sensibles. Ce ne sont pas les données qui révèlent leur caractère sensible, mais leur traitement. Conformément au principe de finalité, c'est la finalité qui fera que le traitement tombe ou ne tombe pas dans le champ d'application de l'article 6, paragraphe (1). En d'autres termes, si la finalité est de traiter des données pour révéler leur caractère sensible, l'interdiction trouvera application. Ce n'est donc pas parce que l'on est en présence de données sensibles que tout traitement est ipso facto interdit<sup>4</sup>.

Par exemple, le traitement d'un chèque adressé à une organisation syndicale et portant la mention „cotisation“ et le traitement par une compagnie aérienne de l'exigence pour un passager d'un repas „kasher“ ne doivent pas poser de problème au regard de l'article 6<sup>5</sup>.

1 Chef d'établissement, membres du conseil d'administration, gérant, mais aussi par exemple chef du personnel, conseiller juridique, portier

2 La matière à régler l'est d'ailleurs aussi

3 La „vie sexuelle“, terme utilisé dans la directive, inclut l'orientation sexuelle

4 C'est pourquoi l'utilisation des termes „traitement de données sensibles“ peut prêter à confusion. S'agissant cependant d'un terme souvent utilisé, comme c'est le cas des termes „protection des données“ (voir supra), nous continuerons à les utiliser

5 On suppose que les conditions de légitimité et de qualité des données sont remplies

Si le traitement de données révélant une appartenance syndicale ou les opinions religieuses était interdit, les traitements mentionnés ci-avant seraient prohibés. Or telle n'a pas été l'orientation du projet de loi. Dans ces deux exemples précités, la finalité du traitement n'est pas axée sur la sensibilité des données.

Est par contre prohibé un traitement visant à répertorier des passagers de confession juive en fonction de l'exigence d'un repas „kasher“. De même est interdit tout traitement utilisé par l'employeur pour distinguer les salariés qui sont syndiqués de ceux qui ne le sont pas.

Les données sensibles peuvent être traitées dans les hypothèses suivantes:

- a. „La personne concernée a donné son consentement à un tel traitement, sauf indisponibilité du corps humain et sauf le cas interdit par la loi.“ (article 6, paragraphe (2) lettre (a))
- b. „Le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement notamment en matière de droit du travail dans la mesure où il est autorisé par la loi.“ (article 6, paragraphe (2) lettre (b))
- c. „Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement.“ (article 6, paragraphe (2) lettre (c))
- d. „Le traitement est mis en oeuvre, avec le consentement de la personne concernée par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, dans le cadre de leurs activités légitimes, à condition que le traitement se rapporte aux données nécessaires des seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées.“ (article 6, paragraphe (2) lettre (d))
- e. „Le traitement porte sur des données manifestement rendues publiques par la personne concernée.“ (article 6, paragraphe (2) lettre (e))
- f. „Le traitement mis en oeuvre conformément aux règles de procédures judiciaires en matière civile applicables est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice s'il est mis en oeuvre à cette fin exclusive.“ (article 6, paragraphe (2) lettre (f))

Sont uniquement visées les procédures judiciaires en matière civile<sup>1</sup>. Les procédures pénales sont mentionnées à l'article 6, paragraphe (3)<sup>2</sup>. Ainsi, l'établissement d'une filiation par recoupement de séquences génétiques tombe sous la lettre (f) de l'article 6, paragraphe (2), alors que si des séquences génétiques servent à rechercher ou à confondre l'auteur d'un meurtre ou d'un viol, c'est l'article 6, paragraphe (3) qui s'appliquera. Comme nous le verrons au point par la suite, les paragraphes (2) lettre (f), et (3) de l'article 6 s'appliquent également au traitement des données génétiques

- g. „Le traitement s'avère nécessaire pour un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques sans préjudice de l'application de l'article 7 [du projet de loi] et que ce traitement est mis en oeuvre conformément au régime d'autorisation préalable de la Commission nationale tel que prévu à l'article 14 [de ce même projet de loi].“ (article 6, paragraphe (2) lettre (g))
- h. „Le traitement est mis en oeuvre par voie de règlement grand-ducal tel que prévu à l'article 17 [du projet de loi].“ (article 6, paragraphe (2) lettre (h))
- i. Le principe de l'interdiction du traitement de données sensibles „ne s'applique pas lors d'une procédure judiciaire ou d'une enquête pénale. Toutefois les données génétiques ne peuvent être traitées que pour vérifier l'existence d'un lien génétique dans le cadre de l'administration de la preuve en justice, pour l'identification d'une personne, la prévention ou la répression d'une infraction pénale déterminée.“ (article 6, paragraphe (3))
- j. En vertu du paragraphe (4) de l'article 6, les données génétiques peuvent faire l'objet d'un traitement:
  - dans des cas visés par les articles 6, paragraphe (2) lettres (c) (intérêts vitaux de la personne concernée), (f) (procédures judiciaires en matière civile), (g) (motif d'intérêt public), (h) (autorisation par voie réglementaire), 6 paragraphe (3) (procédures pénales) et 7 (données traitées par les services de la santé), et

<sup>1</sup> Les procédures d'arbitrages sont exclues

<sup>2</sup> Voir point i. ci-après

- lorsque „la personne concernée a donné son consentement et si le traitement est effectué dans les seuls domaines de la santé ou de la recherche scientifique sauf indisponibilité du corps humain et dans le cas où la loi prévoit que l’interdiction visée au paragraphe (1) ne peut être levée par le consentement de la personne concernée“.

k. Le traitement de certaines catégories de données par les services de la santé est régi par l’article 7.

Les conditions posées par l’article 7 sont les suivantes:

- Le traitement doit être „nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l’administration de soins ou de traitements ou de la gestion de services de santé, de la recherche scientifique dans le domaine de la biologie<sup>1</sup> et de la médecine“.
- Le traitement doit être effectué par une instance médicale. L’article 2, lettre (i), définit l’instance médicale comme „tout praticien de la santé et toute personne soumise à la même obligation de secret professionnel, ainsi que tout établissement hospitalier visé par la loi du 28 août 1998 sur les établissements hospitaliers, effectuant un traitement de données nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l’administration de soins ou de traitements ou de la gestion de services de santé“.
- Le traitement peut aussi être effectué „par les organismes de sécurité sociale et les administrations qui gèrent ces données en exécution de leurs missions légales et réglementaires, par les entreprises d’assurance, les sociétés gérant les fonds de pension, la Caisse médico-chirurgicale mutualiste et par celles des personnes physiques ou morales bénéficiant d’un agrément dans le domaine médico-social ou thérapeutique en vertu de la loi du 8 septembre 1998 réglant les relations entre l’Etat et les organismes oeuvrant dans les domaines social, familial et thérapeutique désignées par règlement grand-ducal“. La commission a décidé d’inclure les „entreprises d’assurance, les sociétés gérant les fonds de pension et la Caisse médico-chirurgicale mutualiste“ dans les prévisions de l’article 7, paragraphe (1), sous peine de leur interdire toute activité. En revanche, afin d’éviter des abus, la commission a repris la proposition faite par le Conseil d’Etat dans son avis complémentaire de supprimer le terme trop vague de „mutuelles“. Cependant la commission, tout en partageant les craintes du Conseil d’Etat à propos des personnes oeuvrant dans le domaine ASFT, a décidé de limiter les personnes autorisées à traiter des données sensibles en exigeant leur énumération limitative dans un règlement grand-ducal.

La simple collecte de données relatives à la santé tombe sous le champ de la loi et ne peut être pratiquée que par un organisme à ce autorisé à l’article 7. Or lesdits organismes ne sauraient fonctionner et verser des pensions d’invalidité sans disposer de données relatives à la santé. Dans ces situations, l’article 7 précise que le responsable du traitement doit être soumis au secret professionnel.

- Le traitement doit avoir été préalablement autorisé par la Commission nationale. Ne sont soumis qu’à notification le traitement mis en oeuvre conformément à l’article 36 de la loi du 28 août 1998 sur les établissements hospitaliers ainsi que le traitement mis en oeuvre par un médecin et concernant ses patients<sup>2</sup>.

Un règlement grand-ducal déterminera les conditions dans lesquelles les données concernées pourront être communiquées à des tiers ou être utilisées à des fins de recherche scientifique. La communication induite à des tiers tombe sous le coup de la sanction pénale prévue à l’article 7, paragraphe (5).

## 2. *Le traitement de données judiciaires*

Les données judiciaires, c’est-à-dire les données traitées dans le cadre d’enquêtes pénales ou de procédures judiciaires civiles ou administratives ne peuvent faire l’objet d’un traitement que dans les conditions du droit commun de la procédure pénale, civile ou administrative. Les traitements de données sensibles restent régis par l’article 6 du projet de loi.

Les données relatives aux infractions, condamnations pénales ou mesures de sûreté, y compris dans le cadre de la protection de la jeunesse, doivent être traitées en exécution d’une disposition légale<sup>3</sup>.

1 Y compris de la biotechnologie

2 Article 7, paragraphe (3)

3 Y compris une disposition figurant dans un règlement grand-ducal

Conformément à l'article 8, paragraphe 5., de la directive et de l'article 8, paragraphe (3) du projet de loi, le casier judiciaire reste sous le contrôle du Procureur général d'Etat, autorité publique compétente en la matière<sup>1</sup>.

### 3. *La liberté d'expression*

Dans son avis du 29 janvier 2002, le Conseil d'Etat avait suggéré de reporter l'examen de l'article 9 de la directive lors de la discussion sur le projet de loi concernant la liberté dans les moyens de communication de masse. Il s'agissait pour le Conseil d'Etat d'une matière dans laquelle l'arbitrage entre la liberté d'expression et le droit à la vie privée est d'autant plus délicat que la marge de manœuvre des Etats membres reste importante.

La commission a cependant décidé de maintenir l'article 9 dans le projet de loi, puisque le Luxembourg se doit de transposer la directive qui précise explicitement dans son article 9 que „les Etats membres prévoient, pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations au présent chapitre, au chapitre IV et au chapitre VI dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression“. L'article 9 de la directive impose aux Etats membres une obligation. Il ne s'agit pas d'une faculté. Retirer l'article 9 du projet de loi signifierait une transposition incomplète de la directive.

L'article 9 s'applique aux traitements mis en œuvre aux seules fins de journalisme ou d'expression artistique ou littéraire. La future loi sur la liberté dans les moyens de communication de masse va prévoir des dispositions particulières uniquement en cas de traitement mis en œuvre aux fins de journalisme. Ainsi, par exemple, pourra-t-elle fixer les modalités dans lesquelles seront exercés les pouvoirs de la Commission nationale. Le paragraphe (3) de l'article 9 a été supprimé, alors qu'il s'agissait d'une disposition qui ne concernait uniquement le domaine du journalisme et n'était en aucune relation avec les formes d'expression artistique ou littéraire pourtant également visées par l'article 9.

Aucune définition n'a été donnée pour les termes de „journalisme ou d'expression artistique ou littéraire“. La doctrine belge privilégie un concept fonctionnel de ces notions. C'est en effet non une catégorie professionnelle que la directive, et par conséquent, le projet de loi veulent réglementer, mais certains traitements de données effectués dans le cadre du journalisme et d'une forme d'expression artistique ou littéraire<sup>2</sup>. Tant la directive que le projet de loi font référence au „traitement mis en œuvre aux seules fins de journalisme ou d'expression artistique ou littéraire“. Par conséquent, „il s'agit d'exempter certains traitements dont la finalité est la production en vue de la communication au public d'une expression dont la prétention esthétique, intellectuelle ou d'information sur l'actualité est affirmée. A ce propos, le responsable du traitement ne sera pas forcément un journaliste, un écrivain ou un artiste mais l'organe de presse, l'éditeur, etc.“<sup>3</sup>.

Quelles sont les dispositions du présent projet de loi auxquelles il a été dérogé?

D'abord, en application de l'article 9, paragraphe (1) lettre (a), le traitement n'est pas soumis à la prohibition de traiter les données sensibles prévue à l'article 6, paragraphe (1) ni aux dispositions de l'article 8 „lorsque le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou à des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée“. Par exemple, l'appartenance d'un ministre, d'un député ou d'un candidat à une élection à un parti politique déterminé tombe manifestement sous l'emprise de cette disposition.

Ensuite, un transfert de données vers un pays tiers peut avoir lieu, nonobstant le fait que ce pays tiers n'offre pas le niveau de protection adéquate exigé par l'article 18, paragraphe (1).

Puis l'article 9, paragraphe (1) lettre (c), dispose que l'obligation d'information de l'article 26, paragraphe (1), n'est pas applicable „lorsque son application compromettrait la collecte des données auprès de la personne concernée“.

De même, en vertu de la lettre (d), il est dérogé à l'obligation d'information visée à l'article 26, paragraphe (2), „lorsque son application compromettrait soit la collecte des données, soit une publication en

<sup>1</sup> Article 1er du règlement grand-ducal modifié du 14 décembre 1976 portant réorganisation du casier judiciaire

<sup>2</sup> Léonard, Pouillet, op. cit., p. 381

<sup>3</sup> Ibid. eod. loc.

projet, soit la mise à disposition du public, de quelque manière que ce soit de ces données ou fournirait des indications permettant d'identifier les sources d'information“.

Enfin, l'article 9, paragraphe (1) lettre (e), aménage le droit d'accès de la personne concernée „qui peut être différé ou limité conformément à l'article 28, paragraphe (4) et à l'article 29“. Il s'agit ici d'une dérogation facultative. L'article 29, paragraphe (1) lettre (g), du projet de loi permet au responsable du traitement de limiter ou de différer l'accès aux données, de même qu'aux informations sur leur origine, en se prévalant de la liberté d'expression. Le droit d'accès de la personne concernée „peut être différé ou limité“, mais ne doit pas l'être. La décision incombera au responsable du traitement qui devra apprécier l'opportunité de cette dérogation. En vertu de l'article 28, paragraphe (4), si le droit d'accès a été refusé et si les données en cause n'ont pas encore été publiées, la personne concernée devra demander à la Commission nationale d'avoir accès à ces données ainsi qu'aux informations disponibles sur leur origine. Cependant le responsable du traitement pourra toujours arguer du secret de ses sources pour refuser la divulgation des origines.

En revanche, même dans le cadre d'un traitement aux seules fins de journalisme ou d'expression artistique ou littéraire, le responsable du traitement devra s'assurer que les autres dispositions du projet de loi, comme par exemple, les conditions de légitimité et de qualité des données prescrites aux articles 4 et 5 sont respectées. L'article 9 n'implique en effet aucune dérogation générale aux dispositions du projet de loi, mais seulement des dérogations spécifiques et limitativement énumérées.

Du point de vue des procédures administratives, le contenu d'une notification est limité aux seuls nom et adresse du responsable du traitement.

#### *4. Les traitements à des fins de surveillance*

La surveillance consiste en „toute activité faisant appel à des moyens techniques en vue de détecter, d'observer, de copier ou d'enregistrer les mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile“<sup>1</sup>.

Le projet de loi détermine les règles applicables à toute forme de surveillance (a.) tout en soumettant la surveillance sur le lieu du travail à un régime particulier (b.).

Il se peut qu'un même traitement tombe dans le champ d'application soit de l'article 10 soit de l'article 11 en fonction de la personne concernée. Par exemple, une caméra dans une grande surface tombe sous le coup de l'article 10 si la personne concernée est un client, même potentiel, du magasin et sous celui de l'article 11 si la personne concernée est un salarié employé par le propriétaire de ce magasin.

Quel que soit le régime applicable, la ratio legis exige que les moyens de surveillance ne soient pas cachés (principe de la transparence).

##### *a. Le régime général*

Depuis quelques années, le nombre de caméras et autres moyens de surveillance dans des lieux tant privés que publics augmente considérablement. Ainsi, par exemple, un habitant de Londres est susceptible d'être filmé en moyenne 300 fois chaque jour par une des nombreuses caméras de surveillance<sup>2</sup>. Afin d'éviter de dégénérer de la société de l'information – concept empreint de liberté – en société du contrôle de l'information, une intervention du législateur s'impose.

La surveillance doit être effectuée conformément aux dispositions de l'article 4 du projet de loi.

Dérogant à l'article 5, les hypothèses dans lesquelles une surveillance peut être effectuée sont au nombre de trois:

- si la personne concernée y a consenti;
- „aux abords ou dans tout lieu accessible ou non au public autres que les locaux d'habitation, notamment dans les parkings couverts, les gares, aéroports et les moyens de transports publics, pourvu que le lieu en question présente de par sa nature, sa situation, sa configuration ou sa fréquentation un risque rendant le traitement nécessaire à la sécurité des usagers ainsi qu'à la prévention des accidents.“

<sup>1</sup> Article 2, lettre (q)

<sup>2</sup> Focus, 15/2002

Le texte initial du projet de loi ne visait que la finalité de la prévention, la recherche, la constatation et la poursuite d'infractions pénales. D'après l'article 17 du projet de loi, les traitements nécessaires à cette finalité sont autorisés par voie réglementaire. Le Conseil d'Etat a donc suggéré de remplacer cette finalité par la „sécurité des usagers“ et „la prévention des accidents“ au motif qu'il fallait prévenir toute insécurité juridique en distinguant les champs d'application respectifs des articles 10 et 17. La commission s'est ralliée à cette manière de voir.

Le texte de l'article 10, paragraphe (1) lettre (b), répond à cette préoccupation. Cependant il serait inexact de faire abstraction de la finalité consistant en la prévention, la recherche, la constatation et la poursuite d'infractions pénales. „Les données recueillies au cours [du traitement à des fins de surveillance] sont donc susceptibles d'un traitement ultérieur dans le cadre général de la politique pénale, mais ne le sont pas nécessairement.“<sup>1</sup> Le projet de loi prévoit d'ailleurs expressément au paragraphe (3) lettres (b) et (c) de l'article 10 que les données collectées dans le cadre d'une activité de surveillance peuvent être communiquées aux autorités publiques agissant dans le cadre de l'article 17, c'est-à-dire que dans le cadre de la prévention, la recherche et la constatation d'infractions pénales, ainsi qu'aux autorités compétentes pour constater ou poursuivre une infraction pénale. La „sécurité des usagers“ ou la „prévention des accidents“ incluent donc la prévention, la recherche, la constatation et la poursuite d'infractions pénales, puisqu'un traitement ultérieur à ces fins est prévu dans le projet de loi.

Ainsi, par exemple, un responsable du traitement peut installer une caméra près d'un distributeur automatique de billets de banque. La finalité de cette surveillance est la sécurité des usagers. Les données recueillies par ce biais pourront toujours être communiquées aux autorités chargées de la prévention, la recherche, la constatation et la poursuite d'infractions pénales.

Sont visés tous les lieux accessibles ou non au public, y compris les bâtiments publics et administratifs, mais à l'exception des lieux d'habitation. Les lieux d'accès privé, parmi lesquels peuvent être rangés les lieux d'habitation sont mentionnés à la lettre (c) de l'article 10, paragraphe (1). La commission n'a donc pas repris la proposition de supprimer la référence aux locaux d'habitation faite par le Conseil d'Etat dans son avis complémentaire du 2 juillet 2002.

- „aux lieux d'accès privé dont la personne physique ou morale y domiciliée est le responsable du traitement.“ Pour ce qui est des personnes morales, doivent être visés non seulement le siège social, mais aussi le siège des succursales et des établissements.

Le champ de vision des caméras servant à surveiller un tel lieu d'accès privé doit naturellement être limité afin de ne pas déborder sur un lieu d'accès public, comme un trottoir ou la voie publique.

En vertu de l'article 10, paragraphe (2), l'information de la personne concernée se fait par le biais de panneaux de signalisation, de circulaires, d'envois recommandés par voie postale ou électronique ou par tout autre moyen approprié. Cette information doit être soit préalable soit concomitante au traitement. Elle s'étend aux abords ou dans tout lieu visé à la lettre (b) du paragraphe (1) et aux lieux d'accès privé de la lettre (c) de ce paragraphe. Si le responsable du traitement entend soumettre l'entrée de son domicile à une surveillance par caméra, il faut qu'il en informe tout visiteur. Il est évident qu'aucune information préalable ou concomitante n'est requise en cas de consentement de la personne concernée.

Pour des raisons pratiques évidentes, l'information de la personne concernée est limitée à l'existence d'une surveillance. Cependant la personne concernée peut demander au responsable du traitement toutes les informations figurant au paragraphe (2) de l'article 26, comme notamment l'identité du responsable du traitement et, le cas échéant, de son représentant, la ou les finalités déterminées du traitement auquel les données sont destinées, les catégories de données concernées ou la durée de conservation des données. L'exigence que ces informations figurent à côté ou en dessous d'une caméra de surveillance aurait été totalement disproportionnée. Si la personne concernée souhaite s'enquérir, par exemple, de la finalité du traitement, une démarche active de sa part sera nécessaire.

Conformément au paragraphe (3), la communication des données recueillies peut avoir lieu:

- à tout tiers si la personne concernée a donné son consentement sauf lorsqu'une telle communication est interdite par la loi;
- aux autorités publiques agissant dans le cadre de l'article 17, paragraphe (1);

<sup>1</sup> Avis du Conseil d'Etat, doc. parl. 4735<sup>6</sup>

- aux autorités judiciaires compétentes pour constater ou poursuivre une infraction pénale et aux autorités judiciaires devant lesquelles un droit en justice est exercé ou défendu. „Les données collectées à des fins de surveillance peuvent être communiquées à toutes les autorités judiciaires et pas seulement aux autorités pénales.“<sup>1</sup>

b. *La surveillance sur le lieu du travail*

L'article 11 précise les conditions dans lesquelles peut être effectué un traitement aux fins de surveillance sur le lieu du travail. Il n'a pas vocation à se substituer au droit du travail qui reste applicable pour tous les aspects qui ne sont pas abordés par cet article ou, par extension, par le présent projet de loi<sup>2</sup>.

La première question qui s'est posée est celle de savoir si l'on devait inclure dans le projet de loi une disposition réglementant la surveillance sur le lieu du travail.

Les chambres professionnelles étaient partagées. La Chambre de Travail s'y opposait catégoriquement, la Chambre des Fonctionnaires et Employés Publics soulevait des problèmes d'applicabilité à la fonction publique, la Chambre des Métiers accueillait favorablement le principe d'une réglementation, alors que la position de la Chambre des Employés Privés était plus nuancée<sup>3</sup>.

Dans son avis du 29 janvier 2002, le Conseil d'Etat a suggéré de supprimer l'article 11 et d'approfondir la problématique en la plaçant dans un contexte plus général.

La commission du travail et de l'emploi est convaincue de la nécessité de légiférer en la matière „avec la finalité d'instituer une protection efficace du salarié lui conférant toutes les garanties nécessaires pour faire respecter ses droits dans ce domaine“<sup>4</sup>. La commission partage cette approche en y ajoutant qu'il convient de préciser les droits et obligations tant des salariés que des employeurs.

L'article 11 intervient afin d'éviter des abus et un certain flou juridique préjudiciable pour tous.

Ceci d'autant plus que la jurisprudence de la Cour européenne des droits de l'homme n'a pas limité le droit au respect de la vie privée au seul domicile privé. „Le respect de la vie privée doit aussi englober dans une certaine mesure le droit de l'individu de nouer et de développer des relations avec ses semblables. Il n'y a aucune raison de principe d'en exclure les activités professionnelles ou commerciales.“<sup>5</sup>

La question de la surveillance des salariés sur le lieu du travail n'est pas nouvelle.

Déjà en 1938, la cour d'appel de Paris a condamné le directeur d'un journal pour avoir ouvert des lettres adressées à l'attention personnelle d'un rédacteur<sup>6</sup>.

La jurisprudence française a déjà eu l'occasion de se prononcer sur l'utilisation par le salarié pendant les heures de travail de moyens de télécommunications appartenant à l'employeur. Cette jurisprudence s'est développée dans le cadre de litiges intervenus suite au licenciement du salarié qui avait utilisé le téléphone, le minitel ou l'ordinateur mis à sa disposition par l'employeur pour vaquer à ses tâches professionnelles, mais „détournés“ par lui à des fins privées.

Outre le caractère particulier de chaque cas d'espèce, lié à l'appréciation souveraine des circonstances de fait, le débat s'est surtout concentré sur le caractère licite des preuves apportées par l'employeur. „Si l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps du travail, tout enregistrement, quels qu'en soient les motifs, d'images ou de paroles à leur insu,

1 Conseil d'Etat, avis complémentaire, sub Article 10, dernier alinéa

2 Comme, par exemple, pour la définition du lieu du travail

3 Pour les détails, il est renvoyé aux documents parlementaires afférents. L'avis de la commission du travail et de l'emploi (doc. parl. 4735<sup>7</sup>) fait un résumé des positions des chambres professionnelles

4 Doc. parl. 4735<sup>7</sup> p. 3

5 Arrêt du 23 novembre 1992 Niemietz/Allemagne, A 251/B, voir aussi arrêt du 27 mai 1997 Halford/Royaume-Uni. Dans cette dernière affaire, la Cour européenne des droits de l'homme a jugé que les interceptions de conversations téléphoniques de Madame Halford faites à partir de son lieu de travail constituaient une violation de l'article 8 CEDH. Certains commentateurs ont estimé au regard des circonstances de l'affaire Halford (Madame Halford n'avait pas été informée au préalable de la possibilité pour l'employeur d'intercepter les conversations téléphoniques et aucune restriction sur l'utilisation des téléphones n'avait été édictée) qu'il n'y aurait pas de violation de l'article 8 CEDH si le salarié avait été informé au préalable des possibilités d'interception

6 DH 1938, p. 520, voir aussi Cass. crim. 16 janvier 1992, G. P. 1992, p. 296

constitue un mode de preuve illicite.<sup>1</sup> L'information préalable des salariés sur l'existence de contrôles inopinés ou de moyens de surveillance légitime rend licite le moyen de la preuve. La licéité du moyen de surveillance ne préjuge pas de sa fiabilité<sup>2</sup>.

Dans une affaire récente, la Cour de cassation française a jugé que „le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée; (...) qu'un employeur ne peut dès lors, sans violation de cette liberté fondamentale [qu'est le secret des correspondances], prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur“<sup>3</sup>.

„La Cour de cassation (...) a manifestement entendu préserver un certain espace d'intimité au salarié, sur les lieux mêmes de son travail, dans lequel, pour reprendre les termes des conclusions de l'avocat général, le „citoyen-salarié“ se substitue au „salarié-citoyen“.“<sup>4</sup> Mais tout compte fait, ne s'agit-il pas ici d'une question de preuve illicite? L'employeur ayant administré la preuve de la faute commise par le salarié par des moyens dissimulés cachés au salarié viole lui-même le principe de loyauté exigé par l'article 1134 du Code civil.

Quoi qu'il en soit, les risques d'abus existent. Pour les salariés qui sont détournés de leurs tâches professionnelles suite à une utilisation inconsidérée d'internet ou à un envoi de messages électroniques, avec les dangers inhérents à ces moyens de communication (virus, encombrement des réseaux, blocage de mémoire de l'ordinateur, consultation de sites à caractère pornographique ou pédophile). L'employeur peut, par le biais de traces laissées par l'employé (cookies, disque dur, relevés téléphoniques<sup>5</sup>, caméras cachées), pénétrer la sphère intime du salarié.

On a parlé à ce sujet d'„éthique de la preuve“<sup>6</sup> ou de „morale de la preuve“<sup>7</sup>.

Ces constatations renforcent la nécessité de légiférer en la matière. Une balance entre les différents intérêts doit être trouvée<sup>8</sup>. Une confiance réciproque doit s'installer entre employeur et salariés.

L'article 11 n'est pas le seul instrument juridique pouvant être invoqué en la matière. On peut citer, sans vouloir être exhaustif, l'article 8 de la Convention européenne des droits de l'homme sur le respect de la vie privée et familiale, l'article 28 de la Constitution sur le secret des lettres, la loi du 11 août 1982 concernant la protection de la vie privée et la recommandation R (89) 2 du 18 janvier 1989 du comité des ministres du Conseil de l'Europe sur la protection des données à caractère personnel utilisées à des fins d'emploi. On peut également soulever l'existence d'un recueil de directives pratiques adopté par le Bureau International du Travail le 7 octobre 1996<sup>9</sup>.

Cet article 11 se base sur une convention collective belge No 68 adoptée le 16 juin 1998 „relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail“. Le champ d'application de l'article 11 s'étend quant à lui à tout mode de surveillance et pas seulement celui par caméras.

En vertu de l'article 11, un traitement à des fins de surveillance sur le lieu du travail est soumis aux conditions suivantes<sup>10</sup>:

- 
- 1 Cass. soc. 20 novembre 1991, D.1992, p. 73. La chambre criminelle de la Cour de cassation française a cependant admis des documents obtenus „dans des conditions douteuses“ à titre d'indices dès lors qu'il y a eu débat contradictoire à leur sujet (sur ce dernier point: Gautier, D. 2001, p. 3152, No 11)
  - 2 Colonna, JCP 1995, II, 22514
  - 3 Cass. soc. 2 octobre 2001, D. 2001, p. 3148
  - 4 Weiss, D. 2001, IR, p. 2944
  - 5 Pour les tribunaux français, même en l'absence d'information préalable des salariés, l'employeur est en droit d'administrer la preuve d'un usage important du téléphone à des fins privées par le biais de la facturation détaillée établie par l'opérateur de téléphone (Cass. soc. 11 mars 1998, cité in Bossu, Nouvelles technologies et surveillance du salarié, RJS 2001, p. 665)
  - 6 Chauvy, conclusions sous Cass. soc. 20 novembre 1991, précité
  - 7 Denis, Quelques aspects de l'évolution récente du système des preuves en droit civil, RTDciv. 1977, p. 673
  - 8 Aux Etats-Unis, cette balance penche, pourrait-on en douter?, nettement en faveur de l'employeur. (Waldmeir, US employees find no right to privacy in cyberspace, [www.FT.com](http://www.FT.com) du 12 août 2001)
  - 9 Pour un résumé de ce recueil: CNIL, La cybersurveillance des salariés dans l'entreprise, mars 2001, p. 19
  - 10 Nous n'aborderons pas une nouvelle fois l'exigence que le traitement soit adéquat, pertinent et non excessif au regard de la finalité recherchée. Le principe de la qualité des données de l'article 4 s'applique également aux traitements à des fins de surveillance sur le lieu de travail

- l’employeur doit être le responsable du traitement;
- le traitement doit avoir été préalablement autorisé par la Commission nationale;
- le traitement doit être nécessaire pour poursuivre l’une des finalités suivantes:

- (a) les besoins de sécurité et de santé des travailleurs,
- (b) les besoins de protection des biens de l’entreprise,

Sont visées en première ligne les caméras installées aux entrées et sorties de l’établissement, y compris les entrées du personnel. Relèvent également de la protection des biens de l’entreprise les moyens de surveillance destinés à s’assurer que des virus ne pénètrent pas le réseau d’ordinateurs, que des fichiers professionnels ne soient pas détruits, que le réseau ne soit pas encombré. On peut encore y ajouter les écoutes téléphoniques effectuées par des établissements de crédit et autres professionnels du secteur financier aux fins d’enregistrer les ordres des clients passés par téléphone à condition toutefois que tant le client ait donné son accord à un tel enregistrement et que le salarié ait été informé que les conversations téléphoniques passées par ce téléphone seront enregistrées.

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

La convention collective belge No 68 précise à ce sujet que „si le contrôle porte uniquement sur les machines, il a pour but d’en vérifier le bon fonctionnement“<sup>1</sup>. Ainsi l’accès par un technicien aux ordinateurs des salariés a-t-il pour but d’assurer le bon fonctionnement du système.

- (d) le contrôle temporaire de production ou des prestations du travailleur, lorsqu’une telle mesure est le seul moyen pour déterminer la rémunération exacte.

Il ne doit y avoir aucun autre moyen pour déterminer la rémunération exacte du salarié, par exemple en cas de travail à la tâche. Le projet de loi est à cet égard plus restrictif que la convention collective dont il s’inspire. En outre il ne peut s’agir que d’un contrôle temporaire.

- (e) dans le cadre d’une organisation de travail selon l’horaire mobile conformément à la loi.

Il s’agit de tenir compte des spécificités de la loi „PAN“ et des dispositions applicables à la fonction publique.

Les finalités étant limitativement énumérées, l’employeur ne saurait détourner les données recueillies pour une autre finalité incompatible avec celle qu’il entendait poursuivre initialement et qu’il a communiquée aux parties concernées en application de l’article 11, paragraphe (2).

Est-ce que l’employeur peut utiliser les données recueillies dans le cadre d’un traitement légitime sur le lieu du travail à l’appui d’un licenciement?

Dès lors que les données ne sont pas détournées de leur finalité, elles peuvent être utilisées en justice. Si, par exemple, des moyens de surveillance ont été installés en vue de la protection des biens de l’entreprise et qu’il appert des données qu’un salarié a porté atteinte à la propriété de l’entreprise en commettant, par exemple, un vol, la finalité n’a pas été détournée. Cette réponse ne concerne que la loyauté de la preuve et non sa fiabilité ou sa pertinence.

Dans les cas visés aux lettres (a), (d) et (e) de l’article 11, paragraphe (1), le comité mixte d’entreprise, s’il y en a un, a un pouvoir de décision tel que défini à l’article 7 paragraphes (1) et (2) de la loi modifiée du 6 mai 1974 instituant des comités mixtes dans les entreprises du secteur privé et organisant la représentation des salariés dans les sociétés anonymes. La commission du travail et de l’emploi relève, à juste titre, que les autres finalités ne rentrent pas dans le domaine de compétence du comité mixte d’entreprise. Il a été décidé de ne pas modifier la loi du 6 mai 1974 en vue d’étendre le domaine de cogestion pour les raisons évoquées dans l’avis de la commission du travail et de l’emploi<sup>2</sup>. En outre les matières visées aux lettres (b) et (c) relèvent de la responsabilité de l’employeur qui doit garder le pouvoir de décision sur l’organisation de l’entreprise.

En raison du lien de subordination entre l’employeur et le salarié – personne concernée, l’article 11 précise que le consentement de ce dernier ne rend pas légitime le traitement mis en oeuvre par l’employeur.

1 Article 4 de la convention collective. A noter que celle-ci s’applique également au contrôle du processus de production portant sur les travailleurs

2 Doc. parl. 4735<sup>7</sup>, p. 4

Suivant en cela les principes dégagés par la jurisprudence française sur la loyauté des modes de preuves, le paragraphe (2) de l'article 11 dispose que doivent être informés préalablement par l'employeur la personne concernée, ainsi que

- pour les personnes tombant sous l'empire de la législation sur le contrat de droit privé: le comité mixte ou à défaut la délégation du personnel ou à défaut encore l'Inspection du travail et des mines; et
- pour les personnes tombant sous l'empire d'un régime statutaire: les organismes de représentation du personnel tels que prévus par les lois et règlements afférents.

L'article 32, paragraphe (6) indique que la personne concernée ainsi que les organes précités peuvent saisir la Commission nationale s'ils estiment que l'employeur n'a pas respecté les dispositions de l'article 11. En raison de la sensibilité de cette matière, qui pourrait envenimer la situation au sein de l'entreprise, la Commission nationale doit statuer dans le mois de sa saisine. L'action en cassation leur est aussi ouverte dans les conditions de l'article 39. Mais, pour les raisons avancées par le Conseil d'Etat dans son avis complémentaire du 2 juillet 2002, l'inopposabilité à la Commission nationale du secret professionnel auquel le responsable du traitement est astreint n'a pas été étendue à la Commission nationale saisie en vertu de l'article 32, paragraphe (6).

Pour terminer, il convient de signaler l'existence d'un document travail adopté le 29 mai 2002 par le groupe institué par l'article 29 de la directive<sup>1</sup>. Il s'agit là d'un document important qui synthétise les réflexions de ce groupe de travail sur la surveillance des modes électroniques de communication, courriers électroniques et internet, sur le lieu de travail.

Ce document de travail<sup>2</sup> énumère les conditions dans lesquelles l'employeur peut procéder à la surveillance des courriers électroniques et d'internet sur le lieu du travail.

Avant de commencer toute surveillance, l'employeur doit s'assurer que cette surveillance est absolument nécessaire pour une finalité déterminée. Cette surveillance ne doit pas être continue et ne doit être envisagée que dans des circonstances exceptionnelles, comme par exemple, lorsque l'employeur doit protéger ses intérêts en cas d'activité criminelle développée par le salarié, ou pour assurer la sécurité du système (détection de virus).

L'activité de surveillance doit être gouvernée par la transparence, tant à l'égard des autorités<sup>3</sup> et des salariés, voire même à l'égard des tierces personnes<sup>4</sup>. L'information des salariés doit être claire, précise et exacte<sup>5</sup>. Les circonstances dans lesquelles la surveillance a lieu doivent être décrites avec précision, comme par exemple, les conditions dans lesquelles le matériel de l'entreprise peut être utilisé à des fins privées, les conditions de la surveillances (par qui, quand, comment), les conséquences qui pourraient être tirées des résultats de cette surveillance.

Le groupe de travail estime recommandé pour l'employeur d'informer immédiatement le salarié d'un usage non autorisé des moyens de télécommunications et notamment d'internet<sup>6</sup>.

L'employeur ne saurait poursuivre des traitements illégitimes et surveiller des activités ayant trait à des données sensibles du salarié.

La surveillance doit être adaptée au but légitime poursuivi. L'employeur doit recourir aux moyens de surveillance les plus protecteurs de la sphère privée du salarié. Le respect de ce principe de proportionnalité exige que, par exemple, doivent être évitées les surveillances automatiques et continues des salariés. De même la surveillance du contenu des courriers électroniques peut être disproportionnée, alors que l'employeur peut se limiter à surveiller les temps d'utilisations, le nombre de courriers électroniques ou la taille des annexes.

1 Les missions de ce groupe sont énumérées à l'article 30 de la directive et à l'article 14 de la directive 97/66/CE. Pour un aperçu de ses activités: voir son 5ème rapport annuel (année 2000) adopté le 6 mars 2002: [www.europa.eu.int/comm/internal\\_market/fr/dataprot/wpdocs/index.htm](http://www.europa.eu.int/comm/internal_market/fr/dataprot/wpdocs/index.htm)

2 Dont seulement une version anglaise est disponible sur le site internet précité

3 L'article 11 exige d'ailleurs une autorisation préalable de la Commission nationale

4 Par exemple, indication standard sur un courrier électronique adressé à une personne extérieure à l'entreprise que la réponse peut faire l'objet d'une mesure de surveillance

5 On peut par exemple penser par une stipulation insérée dans le contrat de travail

6 Par un message d'alerte qui s'affiche sur l'écran d'ordinateur

Des techniques permettent de limiter ou de bloquer l'accès à internet<sup>1</sup>. L'employeur doit également agir avec discernement et tenir compte des possibilités de réponses erronées de moteurs de recherche, de liens erronés ou de publicités trompeuses.

\*

### III. LES DROITS DE LA PERSONNE CONCERNEE

Le chapitre VI du projet de loi traite des droits de la personne concernée. Il s'agit du droit à l'information (A.), du droit d'accès (B.) et du droit d'opposition (C.), lequel n'était pas prévu dans la législation antérieure. S'ajoute encore la question des décisions individuelles automatisées (C.).

#### A. Le droit à l'information

„Le traitement loyal des données suppose que les personnes concernées puissent connaître l'existence des traitements et bénéficier, lorsque des données sont collectées auprès d'elles, d'une information effective et complète au regard des circonstances de cette collecte<sup>2</sup>.“

##### 1. Principe

Deux modalités d'information de la personne concernée sont visées aux articles 10 et 11 de la directive et reprises presque textuellement respectivement aux paragraphes (1) et (2) de l'article 26.

D'abord, lorsque des données sont collectées directement auprès de la personne concernée, le responsable du traitement doit fournir à celle-ci les informations suivantes:

- „(a) l'identité du responsable du traitement et, le cas échéant, de son représentant;
- (b) la ou les finalités déterminées du traitement auquel les données sont destinées;
- (c) toute autre information supplémentaire telle que:
  - les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
  - le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse;
  - l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;
  - la durée de conservation des données.“

Cette information doit avoir lieu au plus tard lors de la collecte des données. Peu importe les moyens et supports employés en vue de la collecte des données, que ce soit, par exemple, par voie de formulaire ou questionnaire standardisé ou non.

Ensuite, en application du paragraphe (2) de l'article 26, lorsque les données n'ont pas été collectées auprès de la personne concernée, que ce soit une personne liée à la personne concernée ou non, le responsable du traitement doit fournir à la personne concernée les informations suivantes:

- „(a) l'identité du responsable du traitement et, le cas échéant, de son représentant;
- (b) la ou les finalités déterminées du traitement auquel les données sont destinées;
- (c) toute information supplémentaire telle que:
  - les catégories de données concernées;
  - les destinataires ou les catégories de destinataires des données auxquels les données sont susceptibles d'être communiquées;
  - l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;
  - la durée de conservation des données.“

<sup>1</sup> Listes noires (listes d'adresses inaccessibles) ou listes blanches (listes d'adresses accessibles)

<sup>2</sup> Directive, considérant 38

Dans ce cas de figure, l'information de la personne concernée a lieu „dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données“, afin de lui permettre de faire usage de ses droits d'accès ou d'opposition.

Quelle que soit la personne qui fournit les données, les précisions suivantes s'imposent:

Il s'agit sans nul doute possible d'une obligation de résultat qui pèse sur le responsable du traitement. Celui-ci n'a pas besoin d'effectuer personnellement la collecte des données, qui peut être faite par des personnes mandatées par lui ou par ses employés<sup>1</sup>. En tout cas, le responsable du traitement ne peut se délier de son obligation en arguant que la collecte a été réalisée par une autre personne. Le responsable du traitement conserve cependant un recours contre la personne qui a fautivement ou intentionnellement négligé d'informer la personne concernée.

L'article 26 fait référence à la collecte des données. Ces termes impliquent la nécessité d'une démarche active du responsable du traitement. Si les données ont été fournies au responsable du traitement par la personne concernée agissant de sa propre initiative, l'article 26, paragraphe (1) ne s'applique pas. Si le responsable du traitement a reçu les données spontanément par quelqu'un d'autre que la personne concernée, l'article 26, paragraphe (2), s'applique.

L'emploi de l'adjectif „déterminées“ pour caractériser les finalités devant être incluses parmi les informations à fournir à la personne concernée vise à éviter que le responsable du traitement n'indique que des finalités vagues, ce qui viderait de son sens le droit à l'information de la personne concernée.

Le responsable du traitement devra fournir toutes les informations supplémentaires nécessaires, compte tenu des circonstances particulières dans lesquelles les données sont collectées, pour assurer à l'égard de la personne concernée un traitement loyal des données, c'est-à-dire une information pleine et entière<sup>2</sup>. La liste de ces informations supplémentaires n'est pas exhaustive. Ainsi, par exemple, si les données n'ont pas été fournies par la personne concernée, celle-ci peut, suivant les cas, être en droit de connaître l'identité de la personne ayant fourni des données la concernant. De même l'article 30, paragraphe (1) lettres (b) et (c), oblige le responsable du traitement à informer la personne concernée de l'existence d'un droit d'opposition en cas de traitement à des fins de prospection.

La personne concernée peut en outre consulter le registre public tenu par la Commission nationale<sup>3</sup>.

La manière dont les informations visées à l'article 26 ont été fournies à la personne concernée importe peu. Il faut cependant que l'information soit lisible et intelligible. Une information orale peut suffire<sup>4</sup>. En cas de contestation sur l'existence ou l'étendue de l'information fournie à la personne concernée, il appartient au responsable du traitement d'apporter la preuve qu'il a satisfait à son obligation d'information de la personne concernée.

L'information doit être fournie à la personne concernée. Le responsable du traitement ne pourra pas se satisfaire d'une information générale publiée, par exemple, dans la presse. L'information doit être ciblée.

## 2. Exceptions

Une première exception découle de l'article 26. Si la personne concernée a déjà été informée avant la collecte ou dès l'enregistrement des données ou au plus tard lors de la première communication de données, selon l'hypothèse retenue, le droit à information disparaît. Il se peut néanmoins que le responsable du traitement doive encore fournir certaines informations compte tenu du degré d'information préalable de la personne concernée. L'information préalable a pu être incomplète<sup>5</sup>. „Par ailleurs, l'exception ne joue que si la personne concernée est informée, non si elle est raisonnablement supposée être informée.“<sup>6</sup>

Les trois autres exceptions sont répertoriées à l'article 27.

1 Par exemple, des personnes effectuant un sondage ou un recensement

2 Directive, articles 10 et 11, paragraphe 1

3 Article 15

4 Sauf que dans le cas d'une information orale, un problème de preuve peut se poser

5 Léonard, Poulet, op. cit., p. 389

6 Ibid., eod. loc.

En premier lieu, le droit de la personne concernée à l'information est écarté, lorsque le traitement est nécessaire pour sauvegarder:

- „(a) la sûreté de l'Etat;
- (b) la défense;
- (c) la sécurité publique;
- (d) la prévention, la recherche, la constatation et la poursuite d'infractions pénales y compris celles à la lutte contre le blanchiment<sup>1</sup>, ou le déroulement de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 [du présent projet];
- (e) un intérêt économique ou financier important de l'Etat ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;
- (f) la protection de la personne concernée ou des droits et libertés d'autrui.“

Ensuite, les impératifs de la liberté d'expression permettent également de déroger aux prescriptions de l'article 26. L'article 9 paragraphe (1), permet de déroger à l'article 26 paragraphe (1) „lorsque son application compromettrait la collecte des données auprès de la personne concernée“ et à l'article 26, paragraphe (2), „lorsque son application compromettrait soit la collecte des données, soit une publication en projet, soit la mise à disposition du public, de quelque manière que ce soit de ces données ou fournirait des indications permettant d'identifier les sources d'information“.

Enfin, d'après le paragraphe (3) de l'article 27, les dispositions de l'article 26 „ne s'appliquent pas lorsque, en particulier pour un traitement ayant une finalité statistique, historique ou scientifique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si l'enregistrement ou la communication des données est prévu par la loi“. Pour mesurer les „efforts disproportionnés“, „peuvent être pris en considération le nombre de personnes concernées, l'ancienneté des données, ainsi que les mesures compensatrices qui peuvent être prises“<sup>2</sup>.

## **B. Le droit d'accès**

Le droit d'accès permet à la personne concernée de s'assurer de l'exactitude des données et des conditions de licéité et de légitimité du traitement.

### *1. Principe*

En application de l'article 28, la personne concernée ou ses ayants droit justifiant d'un intérêt légitime peuvent demander au responsable du traitement:

- „(a) l'accès aux données la concernant;
- (b) la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, sur les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées;
- (c) la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données;
- (d) la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 31.“

L'accès se fait sans frais. Les demandes d'accès peuvent être présentées à des intervalles raisonnables et la communication des informations se fait „sans délais excessifs“.

Que la demande d'accès émane de la personne concernée ou de ses ayants droit, le demandeur doit prouver son identité. S'agissant d'un droit fondamental, le droit d'accès s'exerce sans contrainte, c'est-à-dire sans influence d'un tiers intéressé par les données traitées.

L'article 28, paragraphe (3), a trait aux données concernant un patient et recueillies par une personne exerçant une profession médicale ou un établissement hospitalier. Le droit d'accès aux données le concernant est exercé par le patient lui-même ou par l'intermédiaire d'un médecin qu'il désigne. Le

<sup>1</sup> Voir article 39 de la loi du 5 avril 1993 sur le secteur financier

<sup>2</sup> Directive, considérant 40

droit d'accès pourra encore être exercé, du vivant de la personne concernée, mais placée sous le régime de la curatelle ou sous celui de la tutelle, par l'intermédiaire d'un médecin désigné par son curateur ou tuteur.

L'article 28 indique encore que, si le patient – personne concernée est décédé, le droit d'accès aux données relatives au de jure est exercé par l'intermédiaire d'un médecin désigné par le conjoint non séparé de corps et ses enfants ou par toute personne qui au moment du décès a vécu avec lui dans le ménage ou encore, s'il s'agit d'un mineur, par ses père et mère. Il s'agit de la reprise de l'article 36, alinéa 5, de la loi du 28 août 1998 sur les établissements hospitaliers.

Que se passe-t-il si la personne concernée, qui n'est pas placée sous un régime de protection, est dans l'incapacité physique<sup>1</sup> soit d'exercer elle-même son droit d'accès, soit de désigner un médecin à cette fin? Dans pareille hypothèse, le droit d'accès devrait s'exercer par les mêmes personnes investies du droit d'exercer à la place de la personne concernée le droit d'accès en cas de décès de celle-ci.

Si la personne qui a exercé son droit d'accès a „des raisons sérieuses d'admettre que les données qui lui ont été communiquées ne sont pas conformes aux données traitées“, elle peut en informer la Commission nationale qui procède aux vérifications nécessaires<sup>2</sup>.

Le paragraphe (5) de l'article 28 impose au responsable du traitement de rectifier, effacer ou verrouiller les données qui n'ont pas été traitées en conformité des dispositions du projet de loi, notamment en raison du caractère incomplet ou inexact des données. Faute de ce faire, la Commission nationale peut ordonner l'interdiction temporaire ou définitive du traitement ou la destruction des données. Toute rectification, effacement ou verrouillage doit être notifié sans délai par le responsable du traitement aux destinataires auxquels les données ont été communiquées.

Cette notification exigée par l'article 28, paragraphe (7) et figurant déjà à l'article 23 de la loi du 31 mars 1979, ne doit pas avoir lieu si elle s'avère impossible. „Impossible“ ne signifie pas une notification trop chère ou exigeant des efforts disproportionnés. L'impossibilité vise une impossibilité technique ou matérielle. Ainsi le projet de loi est-il plus restrictif que la directive qui, dans son article 12, lettre c., dispense de la notification non seulement lorsque cela s'avère impossible, mais aussi lorsqu'une telle communication suppose un effort disproportionné. Cette dernière justification pour se dispenser de communiquer aux tiers toute rectification, effacement ou verrouillage n'a pas été reprise dans le projet de loi. La protection des droits de la personne concernée s'en trouve renforcée.

## 2. Exceptions

Les exceptions au droit d'accès sont du même ordre que celles visant le droit à l'information.

Il y a d'une part, la liberté d'expression visée tant à l'article 28, paragraphe (4), qu'à l'article 29, paragraphe (1) lettre (g).

Ensuite, l'article 29, paragraphe (1) énumère les mêmes exceptions que celles figurant à l'endroit de l'article 27, paragraphe (1), en y ajoutant cependant la mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés à l'article 29, paragraphe (1) aux lettres (c) [sécurité publique], (d) [infractions pénales] et (e) [intérêt économique ou financier important].

Le droit d'accès peut aussi être limité, en vertu de l'article 29, paragraphe (2), à condition:

- qu'il s'agisse de données traitées exclusivement à des fins de recherche scientifique ou de données stockées pour une durée n'excédant celle nécessaire à la seule finalité d'établissement de statistiques;
- qu'il n'existe manifestement aucun risque d'atteinte à la vie privée d'une personne concernée;
- que ces données ne puissent être utilisées aux fins de prendre une mesure ou une décision se rapportant à des personnes précises.

En toute hypothèse, le responsable du traitement doit indiquer au demandeur le motif pour lequel il limite ou diffère l'exercice du droit d'accès. Lorsque le droit d'accès est différé, il doit encore indiquer la date à partir de laquelle le droit d'accès peut à nouveau être exercé<sup>3</sup>.

<sup>1</sup> Parce que, par exemple, elle se trouve dans un état comateux

<sup>2</sup> Article 28, paragraphe (6)

<sup>3</sup> Article 29, paragraphe (3)

Le motif de refus de donner accès est notifié par le responsable du traitement à la Commission nationale<sup>1</sup> pour que celle-ci soit à même de remplir sa mission de surveillance et de prendre les mesures qui s'imposent. En effet, au vœu de l'article 29, paragraphe (4), en cas de limitation de l'exercice du droit d'accès, le droit d'accès est exercé indirectement par la Commission nationale. Celle-ci dispose d'un pouvoir d'investigation en la matière et fait opérer la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme au présent projet de loi. L'article 29, paragraphe (4), précise que „la Commission nationale peut communiquer à la personne concernée le résultat de ses investigations, sans toutefois mettre en danger la ou les finalités des traitements en question“.

### C. Le droit d'opposition

Le droit d'opposition est un droit qui n'existait pas sous l'empire de la loi du 31 mars 1979.

Le droit d'opposition peut être invoqué dans les deux cas de figure mentionnés à l'article 30, paragraphe (1).

1. La personne concernée a le „droit de s'opposer à tout moment pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de dispositions légales prévoyant expressément le traitement. En cas d'opposition justifiée, le traitement mis en oeuvre par le responsable du traitement ne peut pas porter sur ces données“ (lettre (a)).

La personne concernée peut s'opposer à ce que des données soient traitées. Elle ne peut s'opposer au traitement en soi, sauf si le traitement est interdit en vertu d'une disposition législative ou réglementaire.

2. La seconde possibilité pour la personne concernée d'exercer son droit d'opposition concerne les traitements réalisés à des fins de prospection<sup>2</sup>.

La personne concernée peut „s'opposer, sur demande et gratuitement, au traitement la concernant envisagé par le responsable du traitement à des fins de prospection; il incombe au responsable du traitement de porter l'existence de ce droit à la connaissance de la personne concernée“ (lettre (b)). Dans cette hypothèse, le droit d'opposition porte sur le traitement et non pas, comme indiqué à la lettre (a), sur la donnée.

Le Conseil d'Etat avait suggéré de supprimer cette disposition, alors qu'elle ferait „dans une large mesure“ double emploi avec l'article 48 de la loi du 14 août 2002 relative au commerce électronique.

La commission a cependant estimé que la suppression de la lettre (b) réduirait la protection de la personne concernée. Dans le cadre de l'article 14 de la directive, la notion de prospection peut recouvrir des significations plus variées que celle visée à l'article 48 de la loi du 14 août 2000. L'article 30 couvre également la prospection à but non commercial.

De plus, conformément à l'article 1er, paragraphe (5) lettre b), et au considérant 14 de la directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information, le commerce électronique est entièrement soumis aux dispositions législatives en matière de protection des données comprises dans les directives 95/46/CE et 97/66/CE.

Enfin, l'article 7, paragraphe (2), de la directive 2000/31/CE ne fait que définir les modalités d'une des deux formes possibles (à savoir l'opt out) du droit d'opposition.

La définition des champs respectifs de ces deux formes (opt in/opt out) est faite par renvoi aux directives 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications et 97/7/CE concernant la vente à distance des biens et des services autres que les services financiers.

Dès lors, la transposition du principe du droit d'opposition visé à l'article 14 de la directive et à l'article 30 du projet de loi ne saurait se satisfaire de l'article 48 de la loi sur le commerce électronique vu son champ d'application et son contenu.

3. La personne concernée a le droit d'être informée „avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospec-

<sup>1</sup> ibid.

<sup>2</sup> Encore appelée „marketing direct“

tion et de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation" (lettre (c)). Le fait de se „voir offrir le droit de s'opposer“ signifie que la personne concernée doit être informée du droit de faire opposition. Cette disposition ne se substitue pas à l'article 26: le responsable du traitement doit indiquer, entre autres, les finalités déterminées poursuivies par le traitement et les tiers qui recevront communication des données collectées.

#### **D. Les décisions individuelles automatisées**

L'article 31 permet à une personne d'être soumise à une décision individuelle automatisée produisant des effets juridiques à son égard, si cette décision:

- „(a) est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telle que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime, ou
- (b) est autorisée par la loi, qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.“

La première hypothèse suppose l'existence d'un contrat (par exemple, credit-scoring).

La seconde hypothèse concerne surtout le secteur public.

Le principe est d'éviter que des décisions automatisées produisent des effets juridiques à l'égard de la personne concernée. Les travaux préparatoires de la loi belge du 11 décembre 1998 commentent cette disposition comme suit: „cette disposition doit éviter que, sans aucune intervention humaine, des décisions sont prises directement sur la base d'un résultat d'un traitement automatisé.“ De même, „on respecte donc la disposition lorsque entre l'obtention du résultat du traitement par ordinateur et la prise de décision il y ait au moins une intervention humaine minimale“<sup>1</sup>.

\*

### **IV. LES FORMALITES DE MISE EN OEUVRE DU TRAITEMENT**

Le mécanisme mis en place par la loi du 31 mars 1979 pêchait par sa lourdeur. Toute banque de données était soumise à autorisation préalable. Le projet de loi sous rubrique introduit une nouvelle philosophie en ce que les banques de données ne sont plus en tant que telles soumises à une quelconque procédure administrative. Ce sont les traitements qui sont visés. En outre, remplaçant la procédure d'autorisation, le projet de loi institue le principe d'une simple notification (A.) tout en maintenant dans des situations particulières notamment lorsque des données susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées, l'obligation d'une autorisation préalable (B.).

Les notifications et autorisations figureront sur un registre public (C.).

#### **A. Le principe: la notification préalable du traitement**

Le principe est posé à l'article 12, paragraphe (1), qui dispose que les traitements font l'objet d'une notification préalable par le responsable du traitement auprès de la Commission nationale. Cette notification préalable au commencement du traitement permet à la Commission nationale d'exercer son contrôle a posteriori, lequel doit être considéré comme „une mesure suffisante“<sup>2</sup> pour la sauvegarde des droits et libertés des personnes concernées.

En application de l'article 13, paragraphe (3), la notification se fait auprès de la Commission nationale moyennant support papier ou informatique suivant un schéma à établir par elle<sup>3</sup>. La Commission nationale accuse réception de la notification. Un règlement grand-ducal, pris sur base des articles 13, paragraphe (5) et 37, paragraphe (4), peut fixer le principe et le montant d'une redevance à payer pour

1 Exposé des motifs, p. 17, cité in Léonard, Poulet, op. cit., p. 391

2 Directive, considérant 52

3 Voir article 43, paragraphe (1)

toute notification ou modification de notification. Cette redevance constitue la contrepartie des frais de personnel et de fonctionnement de la Commission nationale.

Le risque de voir la Commission nationale submergée par une multitude de notifications a amené le législateur à prévoir des aménagements ou dérogations à l'obligation de notification.

D'abord, les traitements relevant d'un même responsable du traitement et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une notification unique<sup>1</sup>. Un traitement poursuivant différentes finalités, à condition que celles-ci soient liées entre elles, ou plusieurs traitements poursuivant la même finalité, peuvent faire l'objet d'une seule et même notification.

Ensuite, la Commission nationale établit et publie des directives<sup>2</sup> en vue d'une notification simplifiée pour les traitements des données dont la mise en œuvre n'est pas susceptible de porter atteinte aux libertés et droits fondamentaux, et notamment à la vie privée, des personnes concernées.

L'article 12, paragraphe (2) précise le contenu de ces directives de notification simplifiée et indique que „les traitements qui correspondent à ces directives font l'objet d'une notification simplifiée de conformité envoyée à la Commission nationale le cas échéant par voie électronique“.

Enfin, conformément aux paragraphes (1) et (3) de l'article 12, sont exemptés de l'obligation de notification:

- a. le traitement effectué en application de l'article 8, y compris le traitement mis en œuvre conformément aux règles de procédures judiciaires en matière civile et nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice;
- b. le traitement qui doit être préalablement autorisé par la Commission nationale (article 14);
- c. le traitement qui doit être autorisé par voie réglementaire (article 17);
- d. le responsable du traitement qui désigne un chargé de la protection des données<sup>3</sup>. Ce chargé de la protection des données établit un registre des traitements effectués par le responsable du traitement et continue ce registre à la Commission nationale;
- e. „le traitement ayant pour seul objet la tenue d'un registre qui en vertu d'une disposition légale est destiné à l'information du public et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime“<sup>4</sup>, comme par exemple le registre du commerce et des sociétés.

Le contenu de la notification est détaillé à l'article 13. Rappelons que, d'après l'article 9, paragraphe (2), en cas de notification d'un traitement réalisé à des fins de journalisme ou d'expression artistique ou littéraire, seuls les nom et adresse du responsable du traitement ou de son représentant sont exigés.

Il va de soi que toute modification de l'une des informations devant figurer dans la notification doit être à son tour notifiée à la Commission nationale.

## **B. L'exception: l'autorisation préalable du traitement**

Cette autorisation découle soit d'une décision de la part de la Commission nationale (1.), soit d'un règlement grand-ducal (2.).

### *1. L'autorisation préalable par la Commission nationale*

Eu égard à l'importance de certaines données ou à leur caractère sensible, une notification préalable ne suffit pas. Constatant que „certains traitements sont susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées, du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, ou du fait de l'usage particulier d'une technologie nouvelle“<sup>5</sup>, la directive permet en son article 20 aux Etats membres de préciser „les traitements susceptibles de présenter des risques particuliers

1 Article 12, paragraphe (1) lettre (b)

2 Le terme de „directive“ a été préféré à celui de „norme“ „afin de ne pas laisser entrevoir que la Commission nationale disposerait en la matière d'un pouvoir réglementaire au sens propre du terme“ (Conseil d'Etat, avis complémentaire, sub Article 12)

3 Voir V. B. 2. ci-après

4 Article 12, paragraphe (3) lettre (b)

5 Directive, considérant 53

au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en oeuvre“.

Présentent ces „risques particuliers“ et sont donc soumis à l’autorisation préalable de la Commission nationale<sup>1</sup>:

- a. les traitements de données sensibles pour lesquels la personne concernée doit donner son consentement (article 6, paragraphe (2) lettre (a))<sup>2</sup>;
- b. les traitements de données sensibles nécessaires pour faire respecter les obligations et droits spécifiques du responsable du traitement, notamment en matière de droit du travail dans la mesure où ce traitement est autorisé par la loi (article 6, paragraphe (2) lettre (b));
- c. les traitements de données sensibles rendues manifestement publiques par la personne concernée (article 6, paragraphe (2) lettre (e));
- d. les traitements de données sensibles nécessaires pour un motif d’intérêt public, notamment à des fins historiques, statistiques ou scientifiques (article 6, paragraphe (2) lettre (g));
- e. les traitements des données génétiques visés à l’article 6, paragraphe (4) lettre (b);
- f. les traitements de données par les services de la santé conformément à l’article 7, paragraphe (1);
- g. les traitements aux fins de surveillance (article 10);
- h. les traitements aux fins de surveillance sur le lieu de travail (article 11);
- i. les traitements de données collectées pour une finalité déterminée, mais destinées à être traitées ultérieurement pour des fins historiques, statistiques ou scientifiques (article 4, paragraphe (2))<sup>3</sup>;
- j. l’interconnexion de données à caractère personnel de l’article 16. Sont visées les interconnexions qui ne sont pas prévues par un texte légal ou réglementaire.

Une interconnexion se définit comme „toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d’autres responsables du traitement“<sup>4</sup>.

Les responsables des traitements en cause doivent présenter une demande conjointe à la Commission nationale aux fins de l’interconnexion. L’interconnexion peut concerner des traitements autorisés par et/ou notifiés à la Commission nationale. Il faudra de toute façon qu’il y ait déjà eu autorisation ou notification. Cependant rien n’interdit une demande d’interconnexion qui soit concomitante avec une ou plusieurs demandes d’autorisation ou une ou plusieurs notifications.

La finalité poursuivie par cette interconnexion est indiquée au paragraphe (2) de l’article 16: „l’interconnexion de données doit permettre d’atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements, ne pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées, être assortie de mesures de sécurité appropriées et tenir compte du type de données faisant l’objet de l’interconnexion.“ La discrimination visée s’entend à la fois d’une discrimination directe que d’une discrimination indirecte.

Les finalités des traitements dont l’interconnexion est demandée doivent être identiques ou liées. La Commission nationale devra également veiller au respect du secret professionnel auquel sont astreintes certaines professions.

La commission estime que l’élaboration de textes législatifs ou réglementaires autorisant une interconnexion de données devra s’inspirer de la ratio des dispositions de l’article 16;

- k. les traitements concernant le crédit et la solvabilité des personnes concernées;

1 Dans son avis complémentaire du 2 juillet 2002, le Conseil d’Etat a donné à considérer si l’on ne devait pas soumettre à autorisation préalable les traitements visés à l’article 6, paragraphe (2) lettre (d), à savoir les traitements mis en oeuvre du consentement de la personne concernée par des organismes à finalité politique, philosophique, religieuse ou syndicale. La commission a décidé de ne pas reprendre la proposition du Conseil d’Etat, dans la mesure où cette extension risquerait d’entrer en conflit avec d’autres libertés fondamentales garanties par la Constitution et la Convention européenne des droits de l’homme

2 Comme l’autorisation doit être préalable au début du traitement, la personne concernée n’a pas pu donner son consentement. Il s’agit donc des traitements auxquels la personne doit consentir, sans que le consentement ait encore pu être obtenu

3 Il est renvoyé au point II. A. 1. a. ci-dessus

4 Article 2, lettre (j)

1. L'utilisation de données à des fins autres que celles pour lesquelles elles ont été collectées. L'article 14, paragraphe (1) lettre (e), précise, conformément au principe de finalité, qu'un „tel traitement ne peut être effectué que moyennant le consentement préalable de la personne concernée“.

A l'instar des notifications uniques de l'article 12, l'article 14, paragraphe (3), permet à la Commission nationale d'autoriser par une décision unique plusieurs traitements qui ont une même finalité, qui portent sur des catégories de données identiques et qui ont les mêmes destinataires ou catégories de destinataires. Dans la mesure où l'autorisation est préalable au commencement du traitement, le responsable du traitement adresse à la Commission nationale un engagement formel de conformité du traitement à la description figurant dans l'autorisation.

Le paragraphe (2) de l'article 14 indique le contenu d'une demande en autorisation. Le parallèle avec l'article 13, paragraphe (1), relatif au contenu d'une notification est évident. Cependant, les dispositions des lettres (e) et (f) ainsi que de la lettre (i) de l'article 14, paragraphe (2) sont plus restrictives qu'à l'article 13, paragraphe (1) lettres (d) et (g). En effet, au regard des risques particuliers des traitements soumis à autorisation au regard des droits et libertés fondamentaux des personnes concernées, il a paru nécessaire de demander des informations plus détaillées sur les données concernées et traitements envisagés ainsi que sur les mesures de sécurité que dans le cadre d'une notification. Les termes „description détaillée“ qui figurent à l'article 14, paragraphe (2) lettres (e) et (i), démontrent l'exigence d'une précision non requise à l'endroit de l'article 13.

## 2. L'autorisation par règlement grand-ducal

Deux catégories de traitements doivent être autorisées par règlement grand-ducal. Elles sont limitativement énumérées à l'article 17, paragraphe (1). Il s'agit:

a. des „traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions pénales qui sont réservés, conformément à leurs missions légales et réglementaires respectives, aux organes du corps de la police grand-ducale, de l'Inspection générale de la police et de l'administration des douanes et accises. Le règlement grand-ducal déterminera le responsable du traitement, la condition de légitimité du traitement, la ou les finalités du traitement, la ou les catégories de personnes concernées et les données ou les catégories de données s'y rapportant, l'origine de ces données, les tiers ou les catégories de tiers auxquels ces données peuvent être communiquées et les mesures à prendre pour assurer la sécurité du traitement en application de l'article 22“ du projet de loi. Cette disposition s'inspire de l'article 12-1 de la loi modifiée du 31 mars 1979.

Sur proposition du Conseil d'Etat contenue dans son avis complémentaire, la commission a supprimé de la disposition précitée la „poursuite des infractions pénales“. En effet, comme le note à juste titre le Conseil d'Etat, d'opérer une séparation nette entre les traitements visés à l'article 17 et ceux relevant de l'article 8 dans le champ d'application duquel tombent précisément les actes de poursuite.

b. des „traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique“ et

c. des „traitements de données dans des domaines du droit pénal effectués en vertu de conventions internationales, d'accords intergouvernementaux ou dans le cadre de la coopération avec l'Organisation internationale de police criminelle (OIPC – Interpol)“.

Ces traitements autorisés par règlement grand-ducal peuvent être effectués tant en application d'une disposition de droit interne qu'en application d'une convention internationale.

En raison de la sensibilité des traitements précités, prolongeant le régime de l'article 12-1, paragraphe (4), de la loi du 31 mars 1979, le contrôle et la surveillance de ces traitements ne sont pas exercés par la Commission nationale, mais par une autorité de contrôle ad hoc composée du Procureur Général d'Etat, ou de son délégué qui la préside, et de deux membres de la Commission nationale nommés, sur proposition de celle-ci, par le ministre<sup>1</sup>.

Un règlement grand-ducal déterminera l'organisation et le fonctionnement de cette autorité de contrôle.

L'autorité de contrôle est informée immédiatement de la mise en œuvre d'un traitement de données autorisé par règlement grand-ducal. Elle veille à ce que ces traitements soient effectués conformément aux dispositions légales qui les régissent.

<sup>1</sup> Ce terme est défini à l'article 2, lettre (k)

L'article 17, paragraphe (2) décrit les pouvoirs de cette autorité comme suit:

„Pour l'exercice de sa mission, l'autorité de contrôle a un accès direct aux données traitées. Elle peut procéder, quant aux traitements effectués, à des vérifications sur place et se faire communiquer tous renseignements et documents utiles à sa mission. Elle peut également charger un de ses membres à procéder à des missions de contrôle spécifique qui sont exécutées dans les conditions indiquées ci-dessus.

L'autorité de contrôle fait opérer les rectifications et radiations nécessaires.

Elle présente chaque année au ministre un rapport rendant compte de l'exécution de sa mission.

Le droit d'accès aux données visées au présent article ne peut être exercé que par l'intermédiaire de l'autorité de contrôle. Celle-ci procède aux vérifications et investigations utiles, fait opérer les rectifications nécessaires et informe la personne intéressée que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exécution.“

### C. Le registre public

La Commission nationale tient un registre public sur lequel figurent, conformément à l'article 15, paragraphe (2), les traitements notifiés en vertu de l'article 12, paragraphe (1), les traitements autorisés en application de l'article 14, paragraphe (1) ainsi que les traitements faisant l'objet d'une surveillance par le chargé de la protection des données.

C'est d'ailleurs une des raisons qui explique que le registre tenu par le chargé de la protection des données devra être continué à la Commission nationale<sup>1</sup>.

Ne figurent pas sur ce registre les „traitements ayant pour seul but la tenue d'un registre qui, en vertu d'une loi ou d'un règlement grand-ducal, est destiné à l'information du public et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime“<sup>2</sup>, comme par exemple le registre du commerce et des sociétés.

Au vœu de l'article 15, paragraphe (3), le registre public renseigne les informations devant être communiquées à la Commission nationale dans le cadre de la notification ou de la demande d'autorisation. Partant ces mêmes informations doivent également figurer sur le registre tenu par le chargé de la protection des données.

S'agissant d'un registre public, toute personne peut gratuitement prendre connaissance des informations y figurant. Pour des raisons évidentes, les informations portant sur les mesures de sécurité exigées par les articles 13, paragraphe (1) lettre (g) et 14, paragraphe (2) lettre (i), ne sont pas consultables.

Il est précisé que ce registre est en ligne, ce qui permet une consultation plus aisée.

En application de l'article 15, paragraphe (5), la Commission nationale peut limiter cette publicité „lorsqu'une telle mesure est nécessaire pour sauvegarder:

- (a) la sûreté de l'Etat,
- (b) la défense,
- (c) la sécurité publique,
- (d) la prévention, la recherche, la constatation et la poursuite d'infractions pénales y compris celles à la lutte contre le blanchiment, ou le déroulement de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi,
- (e) un intérêt économique ou financier important de l'Etat ou de l'Union Européenne, y compris dans les domaines monétaire, budgétaire et fiscal,
- (f) la protection de la personne concernée ou des droits et libertés d'autrui,
- (g) la liberté d'expression,
- (h) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points (c), (d) et (e) et

<sup>1</sup> Article 12, paragraphe (3) lettre (a)

<sup>2</sup> Article 15, paragraphe (7)

(i) le secret professionnel et le secret d'affaires de la personne concernée et du responsable du traitement“.

On retrouve ici les limitations similaires au droit d'accès de la personne concernée visées à l'article 29.

\*

## V. LE CONTROLE DU TRAITEMENT

Le contrôle du respect de la conformité des traitements de données aux dispositions du projet de loi est double. D'un côté, il est effectué par un établissement public indépendant, la Commission nationale (A.). De l'autre, un tel contrôle peut se faire en interne, par l'intermédiaire du chargé de la protection des données et en respectant les mesures de sécurité requises (B.).

### A. Le contrôle externe: la Commission nationale pour la protection des données

La commission consultative visée à l'article 30 de la loi du 31 mars 1979 a été rapidement débordée par la tâche qui lui a été confiée. Afin d'assurer un contrôle efficace des dispositions du projet de loi, celui-ci institue une autorité indépendante organisée sous forme d'un établissement public, la Commission nationale. Cette Commission nationale „est un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel“<sup>1</sup>.

Elle est „chargée de contrôler et de vérifier si les données soumises à un traitement sont traitées en conformité avec les dispositions de la présente loi et de ses règlements d'exécution“<sup>2, 3</sup>. Le projet de loi donne à cette autorité tous les moyens nécessaires à une bonne exécution de ses missions afin d'éviter que ne se reproduisent les mêmes problèmes que ceux survenus lors de l'exécution de la loi du 31 mars 1979.

L'échec de la Commission nationale dans l'accomplissement de sa mission signifierait vraisemblablement en même temps l'échec de l'application du projet de loi.

#### 1. Statut de la Commission nationale<sup>4</sup>

La Commission nationale est un établissement public indépendant. Elle est dotée de la personnalité juridique, jouit de l'autonomie financière et administrative et est placée sous l'autorité du membre du gouvernement ayant la protection des données dans ses attributions.

Son siège est fixé à Luxembourg-ville, mais peut être transféré à tout moment dans un autre endroit du Luxembourg par règlement grand-ducal. Le transfert du siège de la Commission nationale est un acte réglementaire, car il affecte l'organisation de la Commission nationale.

La Commission nationale est composée de trois membres effectifs, à savoir un président et deux membres effectifs, et de trois membres suppléants. Ces membres sont nommés par le Grand-Duc sur proposition du Gouvernement en conseil pour un terme de 6 ans, renouvelable une fois. La démission d'un membre de la Commission nationale intervient de plein droit par l'atteinte de la limite d'âge de 65 ans.

Les membres sont révoqués par le Grand-Duc sur proposition du Gouvernement en conseil. L'article 35, paragraphe (7), précise qu'avant toute révocation, la Commission nationale est entendue et pas seulement demandée en son avis. Dans le respect du fonctionnement des institutions, la Commission est obligée de donner son avis et ne saurait bloquer l'application de l'article 35 en retenant de manière déraisonnable son avis. Certes il ne s'agit que d'une consultation, mais le but est d'éviter le risque d'une influence du gouvernement sur la Commission nationale, ce qui remettrait en cause son indépendance.

1 Directive, considérant 62

2 Article 32, paragraphe (1)

3 L'article 17, paragraphe (2) institue un organisme spécifique pour la surveillance des traitements opérés dans le cadre d'une autorisation par voie réglementaire: voir IV. B. 2.

4 Articles 34 à 37

Le successeur d'un membre qui cesse l'exercice de ses fonctions reste en fonction pour la durée du mandat restant à courir.

Tant parmi les membres effectifs que parmi les membres suppléants figurent au moins un juriste et un informaticien justifiant d'une formation universitaire adéquate.

Le président est désigné par le Grand-Duc et prête serment entre les mains du Grand-Duc ou de son représentant. Les autres membres de la Commission nationale prêtent serment entre les mains du président.

Les incompatibilités de fonctions sont mentionnées à l'article 34, paragraphe (3), à savoir „membre du Gouvernement, de la Chambre des Députés, du Conseil d'Etat ou du Parlement Européen“ et l'exercice d'activité professionnelle ou la détention directe ou indirecte d'intérêts dans une entreprise ou tout autre organisme opérant dans le champ des traitements de données.

Le statut des membres effectifs de la Commission nationale est réglé à l'article 24 du projet de loi. Ce statut est calqué sur celui prévu à l'article 9 du projet de loi sur la promotion des droits de l'enfant et la protection sociale de l'enfance<sup>1</sup>.

Les membres suppléants touchent une indemnité dont le montant est fixé par règlement grand-ducal<sup>2</sup>.

La commission nationale est assistée d'agents, d'employés et d'ouvriers<sup>3</sup>. Elle peut recourir à des experts externes engagés sur base d'un contrat de droit privé<sup>4</sup>.

La Commission est un organe collégial. Elle se dote d'un règlement d'ordre intérieur.

Les réunions de la Commission nationale sont convoquées par le président. La Commission nationale doit se réunir à la demande de deux membres effectifs. La convocation est adressée aux seuls membres effectifs et contient l'ordre du jour de la réunion. Si les membres effectifs sont empêchés d'assister à une réunion, ils en avertissent les membres suppléants.

Le quorum de présence est de trois membres. Les décisions sont prises à la majorité des voix, étant entendu qu'il ne saurait y avoir d'abstention. Seuls des votes pour ou contre la proposition figurant à l'ordre du jour sont admissibles.

Aucun membre ne peut assister à une réunion de celle-ci, ni délibérer ni décider dans une affaire où il a un intérêt direct ou indirect. La violation de cette règle fondamentale prescrite à l'article 35, paragraphe (5), entraîne la nullité absolue de la décision prise. Le membre ayant un conflit d'intérêts devra se faire remplacer par un membre suppléant.

La Commission nationale publie chaque année un rapport à l'attention des membres du Gouvernement en conseil. Ce rapport renseigne, entre autres, l'exécution de ses missions et l'état des notifications et des autorisations, les déficiences ou abus qui ne sont pas spécifiquement visés par les dispositions légales, réglementaires et administratives existantes<sup>5</sup>.

S'agissant de l'avis de la CCDH, la commission s'exprime en principe en faveur de l'implication d'une commission consultative des droits de l'homme, dont l'instauration a été demandée par certains représentants des „forces vives de la nation“ afin d'assurer une certaine surveillance de la Commission nationale et un regard critique sur les avis de cette autorité. La CCDH est un organe consultatif du Gouvernement en matière de droits de l'homme qui trouvera ainsi une base légale, alors que son fonctionnement interne actuellement régi par l'arrêté ministériel du 26 mai 2000.

Les dispositions financières, comprenant les obligations de la Commission nationale d'arrêter annuellement son compte d'exploitation et d'établir un budget, sont répertoriées à l'article 37.

---

1 Doc. parl. 4137

2 Article 34, paragraphe (2) dernier alinéa

3 Article 35, paragraphes (1) à (3)

4 Article 36, paragraphe (4)

5 Articles 15, paragraphe (6) et 32, paragraphe (2)

## 2. Missions et pouvoirs de la Commission nationale

D'après l'article 34, paragraphe (1) alinéa 3, la Commission nationale exerce en toute indépendance les missions qui lui sont confiées. Ses membres effectifs et suppléants ne reçoivent aucune instruction de quelque autorité que ce soit<sup>1</sup>.

Les missions et pouvoirs de la Commission nationale sont énumérés à l'article 32, paragraphe (3).

La Commission nationale assure l'application des dispositions du projet de loi et de ses règlements d'exécution en particulier celles relatives à la confidentialité et à la sécurité des traitements.

Elle reçoit les notifications préalables et autorise les traitements. Elle assure la publicité des traitements en tenant un registre afférent dans les conditions de l'article 15.

La Commission nationale est demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement, de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi. Ces avis sont publiés dans son rapport annuel.

La Commission nationale a le droit de présenter au Gouvernement toutes suggestions susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données. Elle conseille le Gouvernement sur les conséquences de l'évolution des technologies de traitement de l'information au regard du respect des libertés et droits fondamentaux des personnes. Pour ce faire, elle peut faire procéder à des études, des enquêtes ou expertises.

Elle reçoit et, le cas échéant après discussion avec les auteurs, approuve les codes de conduite relatifs à un traitement ou un ensemble de traitements lui soumis par des associations professionnelles représentatives de responsables du traitement.

Elle „favorise de façon régulière et par tout moyen qu'elle juge opportun, la diffusion d'informations relatives aux droits des personnes concernées et aux obligations des responsables du traitement, notamment en ce qui concerne le transfert de données vers des pays tiers“<sup>2</sup>.

La saisine de la Commission nationale s'opère par toute personne, agissant par elle-même, par l'entremise de son avocat ou par toute autre personne physique ou morale dûment mandatée afin de faire respecter ses droits et libertés fondamentaux à l'égard d'un traitement. La personne concernée est informée des suites réservées à sa requête.

La personne concernée peut demander à la Commission nationale de vérifier la licéité d'un traitement en cas de refus ou de limitation de l'exercice du droit d'accès de la personne concernée conformément à l'article 29, paragraphe (4).

Si la Commission nationale est saisie par l'une des personnes ou organes visés à l'article 11, paragraphe (2), sur une violation de cet article<sup>3</sup>, elle statue dans le mois de la saisine. Dans les autres cas, la législation sur la procédure administrative non contentieuse s'applique, la Commission nationale étant à considérer comme autorité administrative. Le silence de la Commission nationale pendant une durée de trois mois vaut donc rejet de la demande présentée par la personne concernée ou par les autres personnes mentionnées à l'article 32, paragraphe (4).

La Commission nationale dispose d'un pouvoir d'investigation en vertu duquel elle a accès aux données faisant l'objet du traitement en question et recueille toutes les informations nécessaires à l'accomplissement de sa mission de contrôle. Elle a un accès direct aux locaux autres que les locaux d'habitation où a lieu le traitement ainsi qu'aux données faisant l'objet du traitement et procède aux vérifications nécessaires.

La Commission nationale a le droit d'ester en justice pour faire respecter les dispositions du projet de loi et des règlements grand-ducaux pris dans le cadre de ce projet de loi. Dans les conditions fixées à l'article 39, elle peut saisir le président du tribunal d'arrondissement où le traitement a eu lieu d'une action en cessation. Elle dénonce aux autorités judiciaires les infractions dont elle a connaissance qui pourront déclencher une action publique si l'infraction ainsi dénoncée est sanctionnée pénalement et/ou qui pourront intenter eux-mêmes l'action en cessation prévue par l'article 39.

1 Article 35, paragraphe (8)

2 Article 32, paragraphe (3) lettre (i)

3 Traitements aux fins de surveillance sur le lieu du travail

En vertu de l'article 33, „la Commission nationale peut prendre les sanctions disciplinaires suivantes:

- (a) avertir ou admonester le responsable du traitement ayant violé les obligations lui imposées par les articles 21 à 24;
- (b) verrouiller, effacer ou détruire des données faisant l'objet d'un traitement contraire aux dispositions de la présente loi ou de ses règlements d'exécution;
- (c) interdire temporairement ou définitivement un traitement contraire aux dispositions de la présente loi ou à ses règlements d'exécution;
- (d) ordonner l'insertion intégrale ou par extraits de la décision d'interdiction par la voie des journaux ou de toute autre manière, aux frais de la personne sanctionnée“.

Les sanctions prises par la Commission nationale peuvent faire l'objet d'un recours en réformation suivant l'article 3 de la loi du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif.

Sur le plan international, la Commission nationale coopère avec les autorités de contrôle instituées dans les autres Etats membres de l'Union européenne, dans la mesure nécessaire à l'accomplissement de leurs missions notamment en échangeant toutes informations utiles. La Commission nationale représente le Luxembourg au „groupe de protection des personnes à l'égard du traitement des données à caractère personnel“ institué par l'article 29 de la directive.

## **B. Le contrôle interne**

Ce contrôle interne comporte deux volets. Le premier consiste pour le responsable du traitement de prendre toutes les mesures de sécurité nécessaires pour assurer la sécurité des traitements (1.). Le second est une innovation du projet de loi qui prévoit l'institution d'un chargé de la protection des données (2.).

### *1. Subordination et sécurité des traitements*

L'article 21 dispose que „toute personne qui agit sous l'autorité du responsable du traitement ou sous celle du sous-traitant, ainsi que le sous-traitant lui-même, et qui accède à des données ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales“.

Conformément à l'article 24, paragraphe (1), l'article 458 du Code pénal s'applique aux membres de la Commission nationale et à toute personne qui accomplit une mission pour son compte ainsi qu'au chargé de la protection des données. Cette obligation perdure même après la fin de leur fonction.

Même si le projet de loi ne le prévoit pas expressis verbis, il en va de même pour les responsables du traitement et les personnes visées à l'article 21, alors qu'il s'agit de „personnes dépositaires, par état ou par profession, des secrets qu'on leur confie“. Il en va de même pour toute personne travaillant pour la Commission nationale et ayant accès à des informations confidentielles.

Le projet de loi précise, en son article 24, paragraphes (2) et (3) que le chargé de la protection des données agissant dans le cadre de l'accomplissement de ses missions et le prestataire de service de certification ne peuvent opposer à la Commission nationale le secret professionnel auquel ils sont soumis<sup>1</sup>. De même en vertu du paragraphe (4) de cet article, s'agissant du traitement de données sensibles par les services de la santé prévu à l'article 7, „le responsable du traitement agissant dans le cadre de l'accomplissement de ses missions visées à l'article 7, paragraphe (1), ne peut opposer à la Commission nationale le secret professionnel auquel il est soumis lorsque celle-ci a été saisie conformément à l'article 32, paragraphes (4) et (5)“. La référence à l'article 32, paragraphe (6) a été supprimée sur proposition du Conseil d'Etat et pour les motifs contenus dans son avis complémentaire.

Conformément à l'avis du Conseil d'Etat, il y a lieu d'encadrer l'accès aux données relatives à la santé. Toutefois cet encadrement ne peut consister en une limitation des types de renseignements accessibles. La protection de la vie privée de la personne concernée se limite à la seule hypothèse dans laquelle la Commission nationale agirait de son propre chef. Dès lors qu'elle est saisie sur requête de la personne concernée, rien ne s'oppose à ce que la Commission nationale ait accès aux données du demandeur.

<sup>1</sup> Le secret professionnel du prestataire de service de certification est régi par l'article 19 de la loi du 14 août 2000 relative au commerce électronique

Les règles concernant la sécurité du traitement sont énumérées aux articles 22 et 23.

Eu égard à la nature des données, la sécurité du traitement revête un caractère particulièrement important.

„Le responsable du traitement doit mettre en œuvre toutes les mesures techniques et d’organisation appropriées pour assurer la protection des données qu’il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l’altération, la diffusion ou l’accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite<sup>1</sup>.“

Ces mesures de sécurité doivent être communiquées à la Commission nationale dans le cadre de la notification ou de l’autorisation. En vertu de l’article 15, paragraphe (4), les indications fournies par le responsable du traitement à cette occasion ne seront pas accessibles dans le cadre de la consultation de ce registre.

Les mesures de sécurité font l’objet d’un rapport annuel à soumettre par le responsable du traitement à la Commission nationale.

Les mesures de sécurité doivent également être respectées par toute personne qui agit sous l’autorité du responsable du traitement. A cet effet, le sous-traitant choisi par le responsable du traitement doit apporter „des garanties suffisantes au regard des mesures de sécurité technique et d’organisation relatives aux traitements à effectuer“<sup>2</sup>. Il appartient au responsable du traitement et au sous-traitant de veiller au respect de ces mesures.

Le sous-traitant doit avoir conclu par écrit un contrat ou un autre acte juridique dans lequel il est clairement stipulé, d’une part, que, conformément à l’article 21, il n’agit que sur la seule instruction du responsable du traitement, et d’autre part, que les obligations de sécurité des traitements lui incombent également. Il s’agit là du contenu minimal de cet écrit qui peut détailler les moyens de sécurité à mettre obligatoirement en œuvre par le sous-traitant et préciser les obligations respectives en la matière.

Les mesures de sécurité doivent englober un certain nombre de contrôles spécifiés à l’article 23. Cet article indique que, conformément au principe de proportionnalité, la mise en œuvre de ces contrôles doit être fonction du risque d’atteinte à la vie privée ainsi que de l’état de l’art et des coûts liés à la mise en place et à l’application de ces mesures. Lorsqu’il doit mettre en pratique ce critère de proportionnalité, le responsable du traitement s’attachera d’abord à tenir compte du risque d’atteinte à la vie privée. Le fait que ce critère prime celui lié à l’état de l’art et celui des coûts de mise en œuvre résulte de l’article 1er du projet de loi et, en général, de la ratio legis de l’ensemble du projet de loi.

Les contrôles visés à l’article 23 reprennent ceux énumérés à l’article 118 de la Convention de Schengen. Il s’agit du:

- a. contrôle à l’entrée des installations où sont traitées des données;
- b. contrôle des supports de données pour éviter un accès par une personne non autorisée;
- c. contrôle de la mémoire afin d’empêcher l’introduction non autorisée de toute donnée dans le système d’information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées;
- d. contrôle de l’utilisation;
- e. contrôle de l’accès d’un système de traitement automatisé de données;
- f. contrôle de la transmission;
- g. contrôle de l’introduction pour pouvoir vérifier et constater a posteriori l’identité des personnes ayant eu accès au système d’information et quelles données ont été introduites dans le système, à quel moment et par quelle personne;
- h. contrôle du transport de données;
- i. contrôle de la disponibilité par l’établissement de copies de sécurité.

L’ensemble de ces mesures doit conférer un „niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger“<sup>3</sup>.

1 Article 22, paragraphe (1)

2 Article 22, paragraphe (2)

3 Directive, article 17, paragraphe 2

## 2. Le chargé de la protection des données

Le chargé de la protection des données, dont l'existence s'inspire de l'expérience allemande des „Datenschutzbeauftragten“, peut être nommé par le responsable du traitement. Il n'y a pas d'obligation pour le responsable du traitement de nommer un tel chargé de la protection des données. Le responsable du traitement aura peut-être intérêt à le faire, alors que ce chargé peut se substituer dans certains cas à la Commission nationale et qu'il peut, mieux que la Commission nationale, car plus près du responsable du traitement, conseiller et guider celui-ci dans l'application des dispositions du présent projet de loi. La subsidiarité et parfois la complémentarité du chargé par rapport à la Commission nationale devront permettre de limiter „l'ampleur bureaucratique du contrôle“<sup>1, 2</sup>.

Nous examinerons successivement le statut du chargé de la protection des données, puis ses missions et pouvoirs, étant entendu que l'article 40 permet en son paragraphe (10) à un règlement grand-ducal de fixer les modalités de désignation et de révocation du chargé de protection des données, d'exécution de ses missions, de même que ses relations avec la Commission nationale.

Une fois désigné et pour le temps de ses fonctions, les traitements de données se font sous sa responsabilité. L'ampleur de sa tâche est à la hauteur de l'activité du responsable du traitement.

Le responsable du traitement désigne le chargé de la protection des données et communique l'identité de celui-ci à la Commission nationale. Il n'y a pas de durée maximale pour exercer les fonctions de chargé de la protection des données.

L'article 40, paragraphe (3), prend le soin de préciser que dans l'exercice de ses missions le chargé de la protection des données est indépendant vis-à-vis du responsable du traitement. Il en découle qu'il ne saurait y avoir ni lien de subordination ni contrat de travail entre le responsable du traitement et le chargé de la protection des données. Ce dernier est un prestataire de services indépendant.

En raison de son indépendance, le chargé de la protection des données ne peut être révoqué par le responsable du traitement pour des raisons liées à l'exercice de ses missions, hormis le cas de la violation de ses obligations légales ou conventionnelles<sup>3</sup>.

Qui peut être nommé chargé de la protection des données? Pour répondre à cette question, il convient de se référer à l'article 40, paragraphes (5) à (10).

Le chargé de la protection des données peut être soit une personne physique soit une personne morale. Il doit être agréé par la Commission nationale. Pour ce faire, le candidat à cette fonction doit justifier avoir accompli une formation universitaire en droit, économie, gestion d'entreprise, sciences de la nature, ou informatique. Il doit en outre disposer d'assises financières de vingt mille euros.

Cependant les membres de certaines professions réglementées peuvent être agréés par la Commission nationale sans autre condition. Il s'agit des avocats à la Cour<sup>4</sup>, des réviseurs d'entreprises, des experts-comptables et des médecins. Cette liste peut être complétée par règlement grand-ducal.

En tout cas, la Commission nationale vérifie les qualités de tout chargé de la protection des données. Elle peut s'opposer à tout moment à sa désignation ou à son maintien, lorsqu'il „(a) ne présente pas les qualités requises pour la fonction de chargé de la protection des données; ou (b) est d'ores et déjà en relation avec le responsable du traitement dans le cadre d'autres activités que celle du traitement des données à caractère personnel et que cette relation fait naître un conflit d'intérêts limitant son indépendance“<sup>5</sup>. Par exemple, un avocat qui défend le responsable du traitement dans le cadre d'un litige et le réviseur d'entreprises qui contrôle les comptes annuels de ce responsable ont un conflit d'intérêts manifeste. Il faudra être circonspect avec ceux qui étaient en relation avec le responsable du traitement, mais ne le sont plus au moment où ils sont désignés.

1 Doc. parl. 4735, p. 50

2 A noter qu'un chargé de la protection des données devrait également être institué au sein des institutions communautaires: voir proposition de décision du Parlement européen, du Conseil et de la Commission relative au statut et aux conditions générales d'exercice des fonctions de contrôleur européen de la protection des données (COM(2001) 411 – C5-0384/2001 – 2001/2150(ACI))

3 Article 40, paragraphe (3), lettre (b)

4 Seuls sont donc visés les avocats inscrits à la liste I du tableau de l'Ordre des avocats de Luxembourg ou de Diekirch, à l'exclusion de tous les autres avocats

5 Article 40, paragraphe (8)

Le responsable du traitement dispose de trois jours pour désigner un nouveau chargé de la protection des données si la Commission nationale s'oppose à sa désignation ou à son maintien. En fait, dans la mesure où l'institution de ce chargé n'est pas une obligation pour le responsable du traitement, cette disposition prescrite par le paragraphe (8) de l'article 40 ne s'appliquera qu'en cas de refus opposé par la Commission nationale au maintien du chargé préalablement désigné.

La Commission nationale définit les modalités du contrôle continu des qualités requises à la fonction de chargé de la protection des données.

En ce qui concerne ses missions et pouvoirs, le chargé de la protection des données ne peut intervenir que pour des traitements ayant donné lieu à notification à la Commission nationale. L'article 40, paragraphe (1), précise à ce sujet que le chargé agit „dans le cadre de l'article 12, paragraphe (3) sous (a) et aux fins y visées“. Il ne saurait donc intervenir dans tout traitement nécessitant une autorisation préalable de la Commission nationale, sous peine de lui voir confier un pouvoir de prendre des décisions administratives pouvant faire grief<sup>1</sup>.

Les pouvoirs du chargé de la protection des données sont fixés au paragraphe (2) de l'article 40, à savoir:

- „(a) un pouvoir d'investigation aux fins d'assurer la surveillance du respect des dispositions de la présente loi et de ses règlements d'exécution par le responsable du traitement;
- (b) un droit d'information auprès du responsable du traitement et corrélativement, un droit d'informer le responsable du traitement des formalités à accomplir afin de se conformer aux dispositions de la présente loi et de ses règlements d'exécution.“

En cas de doute, le chargé de la protection consulte la Commission nationale quant à la conformité à la présente loi d'un traitement mis en œuvre sous sa surveillance.

L'article 12, paragraphe (3) lettre (a), précise que le chargé de la protection des données doit établir un registre des traitements effectués par le responsable du traitement qu'il surveille. Ce registre doit être continué à la Commission nationale pour permettre à celle-ci l'exercice de son pouvoir de contrôle. Les traitements mentionnés sur ce registre figureront également sur le registre public organisé par l'article 15.

\*

## VI. LES RECOURS JURIDICTIONNELS

Une procédure exorbitante du droit commun, l'action en cessation, a été instituée afin de faire ordonner la cessation d'un traitement mis en œuvre en violation des dispositions du présent projet de loi (B.). L'existence de cette procédure particulière ne se substitue cependant pas aux actions de droit commun (A.).

### A. Les recours de droit commun

Nous avons déjà abordé les sanctions administratives qui peuvent être prises par la Commission nationale avec une possibilité de recours devant les juridictions administratives. Des sanctions pénales sont également prévues dans le projet de loi.

En ce qui concerne les recours de nature civile, l'article 38 précise clairement que l'action en cessation de l'article 39 n'est pas la seule base qu'une personne lésée par un traitement peut invoquer. Cette personne peut continuer à tenter des recours sur base du droit commun.

„En cas de dommage subi par l'utilisateur d'une base de données du chef d'information inexacte, celui-ci sera le plus souvent amené à agir en responsabilité sur la base du droit commun. En effet, le régime de responsabilité des produits défectueux institué par la directive du 25 juillet 1985 ne s'applique qu'aux dommages „physiques“ causés aux personnes ou aux biens de consommation privés. Or la plupart du temps, le préjudice occasionné sera de type économique en sorte que sa réparation relève du droit commun de la responsabilité contractuelle et délictuelle. Ce dernier peut égale-

<sup>1</sup> Doc. parl. 4735, p. 50

ment être invoqué en cas de dommage corporel étant donné que le régime de la directive ne se substitue pas, mais se superpose, aux règles de droit commun (art. 13 de la directive).<sup>1</sup>

### B. L'action en cessation

L'action en cessation organisée par l'article 39, paragraphe (1). Alors que le texte initial du projet de loi prévoyait une procédure devant la chambre du conseil du tribunal d'arrondissement, la commission a décidé de remplacer cette procédure par une procédure plus ancrée civilement et inspirée de l'article 21 de la loi du 27 novembre 1986 réglementant certaines pratiques commerciales et sanctionnant la concurrence déloyale.

L'action est portée devant le président du tribunal d'arrondissement du lieu où le traitement est mis en œuvre. Le président de cette juridiction peut se faire remplacer par un juge, comme en matière de référés. Contrairement à l'action en cessation de la loi du 27 novembre 1986 et à celle du projet de loi 4921 sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel, l'action en cessation de l'article 39 n'est pas portée devant le président de la chambre commerciale du tribunal d'arrondissement. En effet, les droits que l'action en cessation de l'article 39 vise à protéger sont de nature civile, de sorte qu'une action devant le président du tribunal s'avère plus appropriée.

Le Procureur d'Etat peut saisir le président du tribunal d'une action en cessation lorsqu'il a déclenché une action publique pour violation de la présente loi. D'après le paragraphe (6) de l'article 39, „la suspension provisoire et le cas échéant la fermeture provisoire peuvent être ordonnées indépendamment de l'action publique. La suspension provisoire ou la fermeture provisoire ordonnée par le président du tribunal d'arrondissement, ou par le juge qui le remplace, prend toutefois fin en cas de non-lieu ou d'acquiescement, et au plus tard à l'expiration d'un délai de deux ans à partir de la décision initiale de suspension ou de fermeture“.

La saisine de la juridiction présidentielle intervient sur requête de la Commission nationale, lorsque le responsable du traitement ne s'est pas conformé à une sanction administrative définitive.

Enfin, la personne concernée ne peut intenter directement une action en cessation qu'après avoir d'abord saisi la Commission nationale conformément à l'article 32. Ce n'est qu'en cas d'inaction de la Commission nationale ou en cas de silence gardé par cette autorité pendant un ou trois mois, selon le cas, que la personne concernée peut elle-même agir en justice.

Le schéma de la procédure est simple. La personne concernée se plaint d'abord auprès de la Commission nationale. De deux choses l'une:

Soit la Commission nationale prend une sanction administrative à l'encontre du responsable fautif, qui peut contester cette décision devant les juridictions administratives<sup>2</sup>. Si ce dernier ne respecte pas la décision de la Commission nationale, alors que cette décision a été confirmée par une décision coulée en force de chose jugée ou qu'elle n'a pas été contestée en justice, la Commission nationale peut saisir le président du tribunal d'arrondissement d'une action en cessation.

Soit la Commission nationale ne prend aucune sanction ou garde le silence pendant une certaine durée, alors la personne concernée peut saisir directement la justice.

Il ne doit exister aucune différence quant à la décision à prendre par le président du tribunal d'arrondissement selon le mode de sa saisine.

Le président du tribunal d'arrondissement ordonne la cessation du traitement contraire aux dispositions du présent projet de loi et la suspension provisoire de l'activité du responsable du traitement ou du sous-traitant.

Il peut, mais ne doit pas, ordonner la fermeture provisoire de l'établissement du responsable du traitement ou du sous-traitant lorsque sa seule activité est de traiter des données. Cette fermeture provisoire visée à la dernière phrase de l'article 39, paragraphe (1) n'est que facultative. En outre, pour qu'elle puisse être prononcée, le responsable du traitement ou le sous-traitant mis en cause doit avoir pour activité exclusive le traitement de données, c'est-à-dire être un professionnel en la matière. Des „brebis

1 Montero, La responsabilité civile du fait des bases de données, Travaux de la Faculté de droit de Namur, Presses universitaires de Namur, p. 377, No 187. La directive du 25 juillet 1985 (JOCE du 7 août 1985, L 210/29) a été transposée en droit luxembourgeois par la loi modifiée du 21 avril 1989

2 Article 33, paragraphe (2)

galeuses“ peu respectueuses de la législation ne doivent pas noircir la réputation d’une profession respectable et des mesures draconiennes doivent être envisagées à leur encontre.

En outre, il est opportun de prévoir une sanction contre le sous-traitant, même si ce dernier, au vœu de l’article 21, ne peut procéder à un traitement que sur ordre du responsable du traitement.

Se pose la question de savoir si la fermeture provisoire de l’établissement du sous-traitant pourra être ordonnée même si ce sous-traitant effectue des traitements pour des responsables de traitement autres que le responsable contrevenant. D’après le texte de l’article 39, la fermeture provisoire pourra être ordonnée en pareille hypothèse. Certes le sous-traitant agit sous les ordres du responsable du traitement, mais il a une obligation de veiller à la légalité du traitement et devra s’opposer à des instructions du responsable du traitement, lorsqu’il estime que ces instructions débouchent sur un traitement contrevenant aux dispositions légales ou réglementaires.

Du point de vue procédural, comme dans le cadre de la loi précitée du 27 novembre 1986, l’action est introduite et jugée comme en matière de référé conformément aux articles 932 à 940 du Nouveau code de procédure civile. Toutefois, par dérogation à l’article 939, alinéa 2, du Nouveau code de procédure civile, l’ordonnance de référé n’est pas susceptible d’opposition.

Le paragraphe (2) reprend la jurisprudence édictée sous l’empire de l’article 21 de la loi du 27 novembre 1986 qui admet la recevabilité de l’action en cessation „même lorsque le traitement illégal a pris fin ou n’est plus susceptible de se reproduire“.<sup>1</sup>

Le président du tribunal d’arrondissement peut assortir sa décision d’une astreinte sur base des articles 2059 à 2066 du Code civil.

Il peut ordonner la publication de sa décision, soit en totalité soit par extrait, aux frais du contrevenant. La publication peut être ordonnée par la voie des journaux ou de toute autre manière. Elle ne peut avoir lieu qu’en vertu d’une décision coulée en force de chose jugée, c’est-à-dire après que les délais d’appel aient passé ou qu’un appel ait été vidé. On tempère ainsi les effets de la décision du président du tribunal qui est exécutoire par provision.

Cette procédure va permettre de prendre, dans un délai rapide, des mesures importantes pour le respect des droits et libertés fondamentales de la personne concernée.

\*

## VII. LE TRANSFERT DE DONNEES VERS UN PAYS TIERS

Les articles 18 et 19 régissent les transferts de données vers des Etats non membres de l’Union européenne.

Le projet de loi sous rubrique reprend les dispositions figurant aux articles 25 et 26 de la directive. L’article 18 fixe les principes régissant les flux transfrontaliers en direction de pays tiers (A.), tandis que l’article 19 réunit les dérogations (B.).

### A. Principes

Il aurait été aberrant d’affirmer haut et fort que la directive tend à l’établissement d’un „niveau élevé de protection dans la Communauté“<sup>2</sup> tout en ne tenant pas compte des mouvements internationaux de données et du caractère insatisfaisant d’une protection des personnes concernées dans le pays de destination.

C’est pourquoi le transfert de données vers un pays tiers „ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat et moyennant le respect des dispositions de la présente loi et de ses règlements d’exécution“<sup>3</sup>. Peu importe que les données aient déjà fait l’objet d’un traitement avant leur transfert ou qu’elles aient été collectées en vue d’un traitement dans un Etat tiers.

Par conséquent, comme le relève l’article 18, paragraphe (4), „lorsque la Commission européenne ou la Commission nationale constate qu’un pays tiers ne dispose pas d’un niveau de protection adéquat, tout transfert de données vers ce pays est prohibé“.

1 Cour 19 octobre 1977, Pas. 24, 46, Cour 31 mai 1978, Pas. 24, 127

2 Directive, considérant 10

3 Article 18, paragraphe (1)

Les flux de données entre plusieurs Etats membres de l'Union européenne ne sont pas concernés<sup>1</sup>.

En outre seul l'Etat de la destination finale est pris en compte. Ainsi, si les données collectées au Luxembourg sont d'abord transférées en France, puis aux Etats-Unis, enfin au Canada, le niveau de protection qui sera considéré sera celui existant au Canada.

Qu'est-ce qu'un „niveau de protection adéquat“?

„Ce qui est visé n'est effectivement pas une concurrence „équivalente“ dans le sens où un recopiage mot à mot de la directive serait suffisant: il s'agit bien de vérifier comment, en pratique, les principes fondamentaux de protection des données sont respectés dans les pays tiers (principe de similarité fonctionnelle).“<sup>2</sup>

Pour vérifier ceci, le responsable du traitement doit tenir compte „de toutes les circonstances relatives à un transfert ou une catégorie de transferts de données, notamment la nature des données, la finalité et la durée du ou des traitements envisagés, le pays d'origine et le pays de destination finale, les règles de droit générales et sectorielles en vigueur dans le pays en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées“<sup>3</sup>.

Le groupe prévu à l'article 29 de la directive a établi une méthodologie et des critères d'appréciation du caractère adéquat de la protection<sup>4</sup>. Le responsable du traitement peut légitimement s'inspirer de ces critères.

En cas de doute, il peut saisir la Commission nationale. Ce sera elle qui appréciera si un pays tiers assure un niveau de protection adéquat<sup>5</sup>. La Commission nationale informe la Commission européenne des pays au sujet desquels elle a constaté l'absence d'un niveau de protection adéquat<sup>6</sup>.

L'article 25, paragraphe 6., de la directive permet à la Commission européenne de constater qu'un pays tiers assure un niveau de protection adéquat. L'alinéa 2 ajoute que „les Etats membres prennent les mesures nécessaires pour se conformer à la décision de la Commission [européenne]“.

Donc si la Commission européenne constate qu'un Etat assure un niveau de protection adéquat des personnes, un transfert de données en direction de ce pays ne pose pas de problème.

La Commission européenne a reconnu que les législations suisse, hongroise et canadienne présentaient un niveau de protection adéquat<sup>7</sup>. De même, en vertu d'une décision de la Commission européenne du 26 juillet 2000, la Commission a décidé que les principes de la „sphère de sécurité/safe harbour“ édictés par le ministère américain du commerce remplissent les critères de protection adéquate<sup>8</sup>. Si une société américaine respecte les principes de la „sphère de sécurité“ et adhère au contrat y relatif, elle peut importer des données en provenance, même indirecte, d'un Etat membre de l'Union européenne<sup>9</sup>.

## B. Exceptions

L'article 19 permet dans certaines hypothèses le transfert de données dans un pays tiers qui n'assure pas un niveau de protection adéquat.

Un transfert est possible dans les situations suivantes, reprises telles quelles de l'article 26 de la directive:

- a. la personne concernée a donné son consentement au transfert envisagé,

1 Havelange, Lacoste, op. cit., p. 243

2 Havelange, Lacoste, op. cit., p. 242

3 Article 18, paragraphe (2).

4 Document de travail adopté le 24 juillet 1998; publié sous: [www.europa.eu.int/comm/ internal\\_market/en/data-prot/wpdocs/index.htm](http://www.europa.eu.int/comm/internal_market/en/data-prot/wpdocs/index.htm)

5 Voir article 18, paragraphe (4)

6 L'article 20 institue un mécanisme d'information réciproque entre les autorités luxembourgeoises et la Commission européenne

7 Voir Commission européenne, communiqué de presse du 22 janvier 2002

8 Pour une description de cette décision: Havelange, Lacoste, op. cit., pp. 244 et ss.

9 Pour la liste de ces sociétés: <http://web.ita.doc.gov/safeharbour/shlist.nsf/webPages/safe+harbour+list>

- b. le transfert est nécessaire à l'exécution d'un contrat auquel la personne concernée et le responsable du traitement sont parties ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée,
- c. le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers,
- d. le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice,
- e. le transfert est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou
- f. le transfert intervient depuis un registre public tel que prévu à l'article 12, paragraphe (3) lettre (b).

Le responsable du traitement doit notifier à la Commission nationale un rapport établissant les conditions dans lesquelles il a opéré le transfert vers un pays tiers qui ne satisfait pas au critère de la protection adéquate.

Mais, conformément au paragraphe (3) de l'article 19, „la Commission nationale peut autoriser, sur la base d'une demande dûment motivée, un transfert ou un ensemble de transferts de données vers un pays tiers et n'assurant pas un niveau de protection adéquat, au sens de l'article 18 paragraphe (2), ceci lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes concernées, ainsi qu'à l'exercice des droits correspondants. Ces garanties peuvent résulter de clauses contractuelles appropriées. Le responsable du traitement est tenu de se conformer à la décision de la Commission nationale“.

La Commission européenne a adopté des décisions établissant des clauses-types afin de simplifier la procédure de ceux qui souhaitent transférer des données tout en voulant s'assurer d'un niveau de protection le plus élevé possible<sup>1</sup>. Si les clauses ne sont pas obligatoires pour les sociétés, il s'agit néanmoins d'un instrument pratique afin de se conformer aux prescriptions du paragraphe (3) de l'article 19.

\*

## VIII. DISPOSITIONS PENALES

Les prescriptions légales les plus importantes sont sanctionnées pénalement. Il n'est pas nécessaire d'entrer dans le détail de toutes ces dispositions.

Contentons-nous des quelques remarques suivantes.

D'abord, la grande majorité des infractions sont des infractions matérielles. L'utilisation dans certains cas de l'adverbe „sciemment“ dénote l'exigence d'une intention doléuse et sert à les distinguer des infractions matérielles à l'endroit desquelles cet adverbe n'a pas été inséré. C'est le cas des articles 28, paragraphes (2) et (8), 30, paragraphe (2), et 32, paragraphe (11).

Ensuite, les sanctions prévues pour toutes les infractions sont uniformes, à savoir un emprisonnement de huit jours à un an et/ou une amende de 251 à 125.000 euros. Ceci laisse à la juridiction répressive suffisamment de latitude pour trouver la sanction adéquate. La juridiction répressive peut en outre pour chaque infraction ordonner la cessation du traitement. Cette cessation peut être assorti d'une astreinte, sauf à l'endroit des articles 28, paragraphe (2) et (8), 29, paragraphe (5), 30, paragraphe (2), et 32, paragraphe (1). Ces dispositions „traitent en effet respectivement du droit d'accès et du droit d'opposition de la personne concernée ou encore des missions et pouvoirs de la Commission nationale, matière où il paraît difficile de concevoir le traitement illégal à faire cesser et sanctionner moyennant peine d'astreinte“.<sup>2</sup>

Enfin, les articles 8, paragraphe (4) et 17, paragraphe (3), précisent que ne sont visées que les personnes „agissant à titre privé“. Il faut éviter que les forces de l'ordre soient exposées à des sanctions pénales, si elles agissent en dehors du cadre réglementaire. La sanction pénale devra, à l'évidence, être limitée aux personnes agissant à titre particulier, la surveillance des forces de l'ordre étant assurée par l'autorité de contrôle et les activités des agents relevant du contrôle interne.

\*

<sup>1</sup> Voir décisions de la Commission 2001/491/CE et 2002/17/CE

<sup>2</sup> Deuxième avis complémentaire du Conseil d'Etat, doc. parl. 4735<sup>12</sup>

## IX. UNE DISPOSITION SPECIFIQUE ET EXCEPTIONNELLE: L'ARTICLE 41

La commission partage entièrement le constat que „suite à la libéralisation des télécommunications la présence sur le marché d’une multitude d’opérateurs et de fournisseurs de services a rendu de plus en plus difficile l’identification et la localisation d’une personne pour l’accomplissement d’une mission légale de surveillance (...) ou d’une mission de sauvegarde de la vie humaine par les services de secours“<sup>1</sup>.

S’inspirant de la législation néerlandaise, et afin d’éviter que les autorités et services de secours n’aient chaque fois à contacter chaque opérateur et fournisseur de services, l’article 41 permet, dans des conditions strictes, à certaines autorités et services d’obtenir un certain nombre de renseignements sur les abonnés et utilisateurs de ces opérateurs et fournisseurs.

L’article 41, paragraphe (1), énumère les conditions d’accès à ces données.

Les autorités compétentes visées aux articles 88-1 à 88-4 du code d’instruction criminelle et celles agissant dans le cadre d’un crime flagrant ou dans le cadre de l’article 40 du code d’instruction criminelle peuvent demander à l’Institut Luxembourgeois de régulation („ILR“) d’avoir accès aux données concernant l’identité des abonnés et utilisateurs des opérateurs et fournisseurs de communications électroniques ainsi que des services postaux et des fournisseurs de ces services.

Ces autorités et la centrale n’ont accès qu’aux données relatives à l’identité des abonnés et utilisateurs, à savoir nom, prénoms, adresse et, le cas échéant, l’adresse IP.

L’accès se fait de plein droit et sur requête à adresser à l’ILR.

La centrale des secours d’urgence 112 et la centrale du service d’incendie et de sauvetage de la Ville de Luxembourg<sup>2</sup> accèdent dans les mêmes conditions et modalités que les autorités visées ci-dessus aux seules données concernant l’identité des abonnés et utilisateurs des opérateurs et fournisseurs de communications électroniques. Elles n’ont pas accès aux données des services postaux. La commission ne voit en effet pas l’utilité d’accès à ces données étant entendu que seule une situation d’urgence justifie une demande d’accès émanant desdites centrales.

Une nouvelle fois le principe de finalité gouverne l’accès à ces données. „L’accès de plein droit se limite aux mesures spéciales de surveillance telles que prévues aux articles 88-1 à 88-4 du Code d’instruction criminelle, celles prises en matière de crime flagrant ou dans le cadre de l’article 40 du Code d’instruction criminelle et aux mesures particulières de secours d’urgence prestées dans le cadre des activités de la centrale des secours d’urgence 112 et de la centrale du service d’incendie et de sauvetage de la Ville de Luxembourg.“<sup>3</sup>

Pour permettre cet accès, l’article 41, paragraphe (2) oblige les opérateurs et les fournisseurs à mettre d’office et gratuitement à la disposition de l’ILR les données en question. Ce paragraphe continue comme suit: „Les données doivent être actualisées au moins une fois par jour. L’accès doit être garanti vingt-quatre heures sur vingt-quatre et sept jours sur sept. Un règlement grand-ducal détermine les services de communications électroniques et services postaux pour lesquels les opérateurs et fournisseurs de services doivent mettre à disposition les données ainsi que la nature, le format et les modalités de mise à disposition des données.“

La procédure est entièrement automatisée après autorisation de la Commission nationale. Celle-ci vérifie en particulier la sécurisation du système informatique utilisé. Cette automatisation permettra l’accès à distance par voie de communication électronique.<sup>4</sup>

La précision de l’automatisation s’avère indispensable du fait qu’un traitement „manuel“ d’une requête soumise par fax ou lettre:

- a. présuppose du côté de l’ILR la mise en place d’un dispositif supplémentaire en matière de ressources humaines, et

1 Doc. parl. 4735, p. 51

2 La centrale du service d’incendie et de sauvetage de la Ville de Luxembourg a été ajoutée au motif que ses activités sont similaires voire identiques à celle de la centrale des secours d’urgence 112.

3 Article 41, paragraphe (3)

4 Article 41, paragraphe (4)

- b. crée un problème de responsabilité dans le chef de l'ILR du fait que celui-ci serait amené à apprécier l'origine et l'exactitude de ces requêtes ce qui n'est pas son rôle. L'esprit de l'article 41 est d'offrir un outil technique destiné à avoir plus facilement accès au nom de la personne et à son numéro de téléphone (IP adresse ...) nonobstant les procédures déclenchées préalablement. L'ILR n'est qu'une interface entre opérateurs et données.

\*

## X. DISPOSITIONS TRANSITOIRES ET FINALES; ENTREE EN VIGUEUR

Au vœu de l'article 45, la loi entrera en vigueur le premier jour du quatrième mois qui suit sa publication au Mémorial. Cependant, afin de permettre la mise en place de la Commission nationale le plus rapidement possible, il est prévu que les dispositions régissant l'organisation de celle-ci entrent en vigueur trois jours après publication de la loi au Mémorial.

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

Cependant „pour autant qu'ils ne sont pas contraires aux dispositions de la présente loi, les règlements pris en exécution de la loi modifiée du 31 mars 1979 précitée resteront en vigueur tant qu'ils n'auront pas été remplacés par de nouvelles dispositions“<sup>1</sup>. Il s'agit de combler le vide juridique qui résulterait d'une abrogation expresse des règlements grand-ducaux pris en exécution de la loi modifiée du 31 mars 1979. Les règlements d'exécution, trouvant une base légale suffisante dans le nouveau texte, resteront en vigueur jusqu'à ce qu'il est pourvu à leur remplacement par de nouvelles dispositions. Sont plus particulièrement visés:

- le règlement grand-ducal du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale, pris sur base de l'article 12-1 de la loi de 1979;
- le règlement grand-ducal du 2 octobre 1992 réglementant l'utilisation de données nominatives médicales dans les traitements informatiques; et
- le règlement grand-ducal du 9 août 1993 autorisant la création et l'exploitation d'une banque de données nominatives constituant la partie nationale du système d'information Schengen (N. SIS) dont la base légale est encore constituée par la loi du 3 juillet 1992 portant approbation des accords de Schengen.

La commission n'a pas retenu le régime transitoire proposé par le Conseil d'Etat. Le régime transitoire du projet de loi lui apparaît plus adapté, alors que la loi du 31 mars 1979 doit être abrogée dans son entièreté.

En vertu de l'article 42, paragraphe (1), les responsables du traitement auront deux ans à compter de l'entrée en vigueur de la loi à venir pour conformer les traitements existant dans des fichiers non automatisés ou automatisés antérieurs à ladite entrée en vigueur aux dispositions du chapitre II<sup>2</sup> et du chapitre VI<sup>3</sup>. Le dernier paragraphe de l'article 42 prévoit une exception en ce qui concerne les données conservées uniquement à des fins de recherches historiques. Dans ce cas, une décision devra être prise par la Commission nationale.

Les fichiers visés à l'article 42, paragraphe (1), sont ceux qui auront été autorisés sous l'empire de la loi du 31 mars 1979. Le projet de loi ne vise en effet pas à „régulariser“ des banques de données qui n'auraient, malgré l'obsolescence de cette législation et malgré la philosophie différente du projet de loi, pas été autorisées. Au cas où des banques de données n'auraient pas été autorisées, les responsables du traitement devront procéder à la notification, voire demander l'autorisation préalable, pour les traitements en cause.

La personne concernée peut cependant demander à obtenir avant l'expiration de ce délai biennal, notamment dans le cadre de l'exercice de son droit d'accès, la rectification, l'effacement ou le verrouillage des données incomplètes, inexactes ou conservées de manière incompatible aux fins légitimes poursuivies par le responsable du traitement<sup>4</sup>.

1 Article 45

2 Chapitre intitulé „Conditions de licéité du traitement“, articles 4 à 11

3 Chapitre intitulé „Droits de la personne concernée“, articles 26 à 31

4 Article 42, paragraphe (2)

En vue de la mise en vigueur des dispositions transitoires de l'article 42, l'article 43 prévoit que le schéma de notification prévu à l'article 13, paragraphe (3), devra être établi par la Commission nationale dans les quatre mois de la nomination de ses membres. La date à partir de laquelle ce schéma de notification est disponible auprès de la Commission nationale sera publiée au Mémorial et fera l'objet d'un communiqué de presse aux journaux édités au Luxembourg.

A partir de cette date, les responsables du traitement auront quatre mois pour notifier leurs traitements à la Commission nationale. En vertu du paragraphe (4), le délai de quatre mois est porté à douze mois en ce qui concerne les traitements non automatisés de données contenues ou appelées à figurer dans un fichier.

La commission tient à préciser qu'en cas de discordance entre les dates de publication au Mémorial et dans les journaux, ce sera la date de publication au Mémorial qui fera courir le délai de quatre mois.

Le paragraphe (3) de l'article 43 concerne les traitements autorisés en application de la loi du 31 mars 1979 par règlement grand-ducal ou arrêté ministériel „autorisant la création et l'exploitation d'une banque de données“. Les responsables de tels traitements notifieront ou demanderont l'autorisation de leurs traitements à l'expiration de la durée de validité de l'autorisation octroyée, à moins que pour des raisons de conformité avec les dispositions du projet de loi, ils jugent nécessaire de le faire auparavant.

\*

## CONCLUSION

Au vu de l'expérience malheureuse de la pratique de la loi du 31 mars 1979, le législateur a saisi l'occasion de la transposition de la directive pour réformer de fond en comble la législation relative à la protection des données.

L'intention du législateur a été d'édicter une législation réaliste visant à établir une balance entre les intérêts des responsables du traitement et les droits et libertés fondamentales des personnes concernées.

D'aucuns reprochent au projet de loi l'utilisation de termes vagues et son caractère „fourre-tout“.

La flexibilité nécessaire dans cette matière et les termes utilisés dans la directive ont parfois donné naissance à des termes aux contours certes vagues. Il est en effet difficile de prévoir la portée de l'évolution technologique en la matière. A-t-on d'ailleurs jamais regretté les termes utilisés par exemple à l'endroit des articles 1382 à 1384 du Code civil ou de l'article 496 du Code pénal?

Le respect des libertés et droits fondamentaux commande à regrouper au sein d'un seul texte de loi l'ensemble des dispositions relatives à la protection des personnes à l'égard des traitements de données, même si la transposition de la directive 97/66/EE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications fera l'objet d'un projet de loi séparé.

\*

Compte tenu des remarques qui précèdent, la commission invite la Chambre des Députés à voter le projet de loi dans la teneur suivante:

\*

**PROJET DE LOI**  
**relatif à la protection des personnes à l'égard du traitement**  
**des données à caractère personnel**

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

**Art. 1er. – Objet**

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

**Art. 2. – Définitions**

Aux fins de la présente loi, on entend par:

- (a) „code de conduite“: contributions sectorielles élaborées en vue de la bonne application de la présente loi. Les codes de conduite sont élaborés à l'échelon national ou communautaire par les associations professionnelles et les autres organisations représentatives des responsables du traitement et sont facultativement soumis pour approbation à la Commission nationale ou au groupe de protection des personnes à l'égard du traitement des données à caractère personnel tel qu'institué par l'article 29 de la Directive 95/46/CE;
- (b) „Commission nationale“: la Commission nationale pour la protection des données;
- (c) „consentement de la personne concernée“: toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou statutaire accepte que les données à caractère personnel fassent l'objet d'un traitement;
- (d) „destinataire“: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers; les autorités qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre de l'exécution d'une mission légale d'enquête ou de contrôle ne sont pas considérées comme des destinataires;
- (e) „donnée à caractère personnel“ (ci-après dénommée „donnée“): toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable („personne concernée“); une personne physique ou morale est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique;
- (f) „donnée relative à la santé“: toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques;
- (g) „donnée génétique“: toute donnée concernant les caractères héréditaires d'un individu ou d'un groupe d'individus apparentés;
- (h) „fichier de données à caractère personnel“ (ci-après dénommé „fichier“): tout ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;
- (i) „instance médicale“: tout praticien de la santé et toute personne soumise à la même obligation de secret professionnel, ainsi que tout établissement hospitalier visé par la loi du 28 août 1998 sur les établissements hospitaliers, effectuant un traitement de données nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé;
- (j) „interconnexion“: toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d'autres responsables du traitement;
- (k) „ministre“: le ministre ayant dans ses attributions la protection des données;
- (l) „organisme de sécurité sociale“: tout organisme de droit public ou privé qui assure des prestations, obligatoires ou facultatives, relatives à la maladie, la maternité, la vieillesse, les accidents corporels,

l'invalidité, la dépendance, le décès, le chômage, ainsi que des prestations familiales ou d'aides sociales;

- (m) „pays tiers“: Etat non membre de l'Union européenne;
- (n) „personne concernée“: toute personne physique ou morale, publique ou privée ou groupement de fait, qui fait l'objet d'un traitement de données à caractère personnel;
- (o) „responsable du traitement“: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu des dispositions légales, le responsable du traitement est déterminé par ou en vertu des critères spécifiques conformément aux dispositions légales;
- (p) „sous-traitant“: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données pour le compte du responsable du traitement;
- (q) „surveillance“: toute activité faisant appel à des moyens techniques en vue de détecter, d'observer, de copier ou d'enregistrer les mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile;
- (r) „tiers“: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placés sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilités à traiter les données. Dans le secteur public, on entend par tiers un ministère, une administration, un établissement public, une commune ou un service public autre que le responsable du traitement ou son sous-traitant;
- (s) „traitement de données à caractère personnel“ (ci-après dénommé „traitement“): toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

### **Art. 3. – Champ d'application**

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

(2) Sont soumis à la présente loi:

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

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

(3) La présente loi s'applique au traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, même liées à un intérêt économique ou financier important de l'Etat, sans préjudice des dispositions spécifiques de droit national ou international régissant ces domaines.

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

(5) La présente loi ne s'applique pas:

- au traitement mis en oeuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques

- au traitement de données concernant une personne morale et dont la publication est prescrite par une loi ou un règlement.

## **Chapitre II. – Conditions de licéité du traitement**

### **Art. 4. – Qualité des données**

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

- (a) collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités;
- (b) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;
- (c) exactes et, si nécessaire, mises à jour; toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;
- (d) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées sans préjudice du paragraphe (2) ci-après.

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

(3) Quiconque effectue un traitement en violation des dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

### **Art. 5. – Légitimité du traitement**

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

- (a) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou si
- (b) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, ou si
- (c) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci, ou si
- (d) le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, ou si
- (e) le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou si
- (f) la personne concernée a donné son consentement.

(2) Quiconque effectue un traitement en violation des dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

### **Art. 6. – Traitement de catégories particulières de données**

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

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

- (a) la personne concernée a donné son consentement à un tel traitement, sauf indisponibilité du corps humain et sauf le cas interdit par la loi, ou lorsque
- (b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement notamment en matière de droit du travail dans la mesure où il est autorisé par la loi, ou lorsque
- (c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement, ou lorsque
- (d) le traitement est mis en oeuvre, avec le consentement de la personne concernée par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, dans le cadre de leurs activités légitimes, à condition que le traitement se rapporte aux données nécessaires des seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées, ou lorsque
- (e) le traitement porte sur des données manifestement rendues publiques par la personne concernée, ou lorsque
- (f) le traitement mis en oeuvre conformément aux règles de procédures judiciaires en matière civile applicables est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice s'il est mis en oeuvre à cette fin exclusive, ou lorsque
- (g) le traitement s'avère nécessaire pour un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques sans préjudice de l'application de l'article 7 ci-après et que ce traitement est mis en oeuvre conformément au régime d'autorisation préalable de la Commission nationale tel que prévu à l'article 14, ou lorsque
- (h) le traitement est mis en oeuvre par voie de règlement grand-ducal tel que prévu à l'article 17.

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

(4) Par dérogation à l'article 6, paragraphe (1), les données génétiques ne peuvent faire l'objet d'un traitement que:

- (a) dans les cas visés par les articles 6, paragraphe (2) lettres (c), (f), (g), (h), 6 paragraphe (3) et 7 de la présente loi, ou lorsque
- (b) la personne concernée a donné son consentement et si le traitement est effectué dans les seuls domaines de la santé ou de la recherche scientifique sauf indisponibilité du corps humain et dans le cas où la loi prévoit que l'interdiction visée au paragraphe (1) ne peut être levée par le consentement de la personne concernée.

(5) Quiconque effectue un traitement ou opère une communication à un tiers en violation des dispositions du paragraphe (1) qui précède est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement ou de la communication contraires aux dispositions du paragraphe (1) du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

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

(1) Lorsque le traitement de données tel que défini à l'article 6 paragraphe (1) de la présente loi est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé, de la recherche scientifique dans le domaine de la biologie et de la médecine, le traitement de ces données peut être mis en oeuvre par des instances médicales, ainsi que lorsque le responsable du traitement est soumis au secret professionnel, par les organismes de sécurité sociale et les administrations qui gèrent ces données en exécution de leurs missions légales et réglementaires, par les entreprises d'assurance, les sociétés gérant les fonds de pension, la

Caisse médico-chirurgicale mutualiste et par celles des personnes physiques ou morales bénéficiant d'un agrément dans le domaine médico-social ou thérapeutique en vertu de la loi du 8 septembre 1998 réglant les relations entre l'Etat et les organismes oeuvrant dans les domaines social, familial et thérapeutique, désignées par règlement grand-ducal. Le recours à un sous-traitant est possible dans les conditions prévues à l'article 21.

(2) Le traitement visé ci-dessus fait l'objet d'une autorisation préalable de la Commission nationale.

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

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

(4) Sous réserve que leur traitement soit en lui-même licite au regard des articles 6 et 7, les données y visées peuvent être communiquées à des tiers ou utilisées à des fins de recherche, d'après les modalités et suivant les conditions à déterminer par règlement grand-ducal.

(5) Quiconque effectue un traitement ou opère une communication à un tiers en violation des dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement ou de la communication contraires aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

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

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

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

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

(4) Quiconque, agissant à titre privé, effectue un traitement en violation des dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

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

(1) Sans préjudice des dispositions prévues dans la législation sur la liberté dans les moyens de communication de masse et dans la mesure où les dérogations ci-après s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression, le traitement mis en oeuvre aux seules fins de journalisme ou d'expression artistique ou littéraire n'est pas soumis:

- (a) – à la prohibition de traiter les catégories particulières de données telle que prévue à l'article 6, paragraphe (1);
  - aux limitations concernant le traitement de données judiciaires prévues à l'article 8; lorsque le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou à des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée;
- (b) à la condition de protection adéquate exigée s'agissant des traitements de données faisant l'objet d'un transfert vers un pays tiers telle que prévue à l'article 18, paragraphe (1);
- (c) à l'obligation d'information de l'article 26, paragraphe (1), lorsque son application compromettrait la collecte des données auprès de la personne concernée;

- (d) à l'obligation d'information de l'article 26, paragraphe (2), lorsque son application compromettrait soit la collecte des données, soit une publication en projet, soit la mise à disposition du public, de quelque manière que ce soit de ces données ou fournirait des indications permettant d'identifier les sources d'information;
- (e) au droit d'accès de la personne concernée qui peut être différé ou limité conformément à l'article 28, paragraphe (4) et à l'article 29.

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

**Art. 10. – Traitement à des fins de surveillance**

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

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

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

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

- (a) si la personne concernée a donné son consentement sauf le cas interdit par la loi,
- (b) aux autorités publiques dans le cadre de l'article 17, paragraphe (1), ou
- (c) aux autorités judiciaires compétentes pour constater ou poursuivre une infraction pénale et aux autorités judiciaires devant lesquelles un droit en justice est exercé ou défendu.

(4) Quiconque effectue un traitement en violation des dispositions du paragraphe (1) qui précède est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du paragraphe (1) du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

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

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

- (a) pour les besoins de sécurité et de santé des travailleurs, ou
- (b) pour les besoins de protection des biens de l'entreprise, ou
- (c) pour le contrôle du processus de production portant uniquement sur les machines, ou
- (d) pour le contrôle temporaire de production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte, ou
- (e) dans le cadre d'une organisation de travail selon l'horaire mobile conformément à la loi.

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

salariés dans les sociétés anonymes. Le consentement de la personne concernée ne rend pas légitime le traitement mis en oeuvre par l'employeur.

(2) Sans préjudice du droit à l'information de la personne concernée sont informés préalablement par l'employeur:

- la personne concernée, ainsi que
- pour les personnes tombant sous l'empire de la législation sur le contrat de droit privé: le comité mixte ou à défaut la délégation du personnel ou à défaut encore l'Inspection du travail et des mines;
- pour les personnes tombant sous l'empire d'un régime statutaire: les organismes de représentation du personnel tels que prévus par les lois et règlements afférents.

(3) Quiconque effectue un traitement en violation des dispositions du présent article est puni d'une peine d'emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une des peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

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

#### **Art. 12. – Notification préalable à la Commission nationale**

(1) (a) A l'exception de ceux qui relèvent des dispositions prévues aux articles 8, 14 et 17, les traitements de données font l'objet d'une notification préalable par le responsable du traitement auprès de la Commission nationale.

(b) Les traitements relevant d'un même responsable du traitement et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une notification unique. Dans ce cas les informations requises en application de l'article 13 ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

(2) Pour les traitements des données dont la mise en œuvre n'est pas susceptible de porter atteinte aux libertés et droits fondamentaux, et notamment à la vie privée, des personnes concernées, la Commission nationale établit et publie des directives en vue d'une notification simplifiée.

Ces directives précisent:

- (a) la ou les finalités du traitement faisant l'objet d'une notification simplifiée;
- (b) la ou les catégories de données traitées;
- (c) la ou les catégories de personnes concernées;
- (d) les destinataires ou catégories de destinataires auxquels les données sont communiquées;
- (e) la durée de conservation.

Les traitements qui correspondent à ces directives font l'objet d'une notification simplifiée de conformité envoyée à la Commission nationale le cas échéant par voie électronique.

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

- (a) le responsable du traitement qui désigne un chargé de la protection des données tenu notamment d'assurer, de manière indépendante, l'application des dispositions légales en la matière et d'établir et de continuer à la Commission nationale un registre des traitements effectués par le responsable du traitement conformément aux dispositions relatives à la publicité des traitements telles que prévues à l'article 15;
- (b) le traitement ayant pour seul objet la tenue d'un registre qui en vertu d'une disposition légale est destiné à l'information du public et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime;
- (c) le traitement mis en œuvre conformément aux règles de procédures judiciaires en matière civile et nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice.

(4) Quiconque ne se soumet pas à l'obligation de notification ou fournit des informations incomplètes ou inexacts est puni d'une amende de 251 à 125.000 euros. La juridiction saisie peut prononcer

la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

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

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

- (a) le nom et l'adresse du responsable du traitement, et le cas échéant de son représentant et du sous-traitant;
- (b) la condition de légitimité du traitement;
- (c) la ou les finalité(s) du traitement;
- (d) la description de la ou des catégories de personnes concernées et des données ou des catégories de données s'y rapportant;
- (e) les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
- (f) les pays tiers à destination desquels des transferts de données sont envisagés;
- (g) une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement en application des articles 22 et 23;
- (h) la durée de conservation des données.

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

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

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

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

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

- (a) les traitements prévus aux articles 6, paragraphe (2) lettres (a), (b), (e), (g), 6 paragraphe (4) lettre (b), aux articles 7, paragraphe (1), 10 et 11 de la présente loi;
- (b) les traitements de données à des fins historiques, statistiques ou scientifiques visés à l'article 4, paragraphe (2). La Commission nationale vérifie en particulier si ces traitements ne peuvent être réalisés sur base de données rendues anonymes;
- (c) l'interconnexion de données visée à l'article 16;
- (d) le traitement concernant le crédit et la solvabilité des personnes concernées;
- (e) l'utilisation de données à des fins autres que celles pour lesquelles elles ont été collectées. Un tel traitement ne peut être effectué que moyennant consentement préalable de la personne concernée.

(2) La demande d'autorisation comprend les informations suivantes:

- (a) le nom et l'adresse du responsable du traitement ou de son représentant et le cas échéant du sous-traitant;
- (b) la condition de légitimité du traitement;
- (c) la ou les finalités du traitement;
- (d) l'origine des données;
- (e) la description détaillée des données ou catégories de données ainsi que des traitements envisagés;
- (f) la description de la ou des catégories de personnes concernées;
- (g) les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
- (h) les pays tiers à destination desquels des transferts de données sont envisagés;

- (i) une description détaillée permettant d'apprécier le respect des mesures de sécurité prévues aux articles 22 et 23;
- (j) la durée de conservation des données.

(3) Les traitements qui ont une même finalité, qui portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la Commission nationale. Dans ce cas le responsable de chaque traitement adresse à la Commission nationale un engagement formel de conformité de celui-ci à la description figurant dans l'autorisation.

(4) Quiconque effectue un traitement en violation des dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

#### **Art. 15. – Publicité des traitements**

(1) La Commission nationale tient un registre public des traitements.

(2) Figurent dans ce registre:

- (a) les traitements notifiés à la Commission nationale en vertu de l'article 12, paragraphe (1);
- (b) les traitements autorisés par la Commission nationale en vertu de l'article 14, paragraphe (1); et
- (c) les traitements surveillés par le chargé de la protection des données et continués à la Commission nationale en vertu de l'article 12, paragraphe (3) (a).

(3) Le registre tenu par la Commission nationale contient sur chaque traitement les informations requises respectivement par l'article 13, paragraphe (1) et par l'article 14, paragraphe (2). Pour les traitements soumis à autorisation préalable, le registre renseigne en plus sur l'autorisation émise par la Commission nationale.

(4) Toute personne peut prendre connaissance, et ce gratuitement, des informations contenues dans le registre public qui est en ligne, à l'exception de celles prévues respectivement à l'article 13, paragraphe (1) lettre (g) et à l'article 14, paragraphe (2) lettre (i).

(5) Cependant la Commission nationale peut limiter cette publicité lorsqu'une telle mesure est nécessaire pour sauvegarder:

- (a) la sûreté de l'Etat,
- (b) la défense,
- (c) la sécurité publique,
- (d) la prévention, la recherche, la constatation et la poursuite d'infractions pénales y compris celles à la lutte contre le blanchiment, ou le déroulement de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi,
- (e) un intérêt économique ou financier important de l'Etat ou de l'Union Européenne, y compris dans les domaines monétaire, budgétaire et fiscal,
- (f) la protection de la personne concernée ou des droits et libertés d'autrui,
- (g) la liberté d'expression,
- (h) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points (c), (d) et (e) et
- (i) le secret professionnel et le secret d'affaires de la personne concernée et du responsable du traitement.

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

(7) Le présent article ne s'applique pas aux traitements ayant pour seul but la tenue d'un registre qui, en vertu d'une loi ou d'un règlement grand-ducal, est destiné à l'information du public et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

**Art. 16. – Interconnexion de données**

(1) L'interconnexion de données qui n'est pas expressément prévue par un texte légal doit faire l'objet d'une autorisation préalable de la Commission nationale sur demande conjointe présentée par les responsables des traitements en cause.

(2) L'interconnexion de données doit permettre d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements, ne pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées, être assortie de mesures de sécurité appropriées et tenir compte du type de données faisant l'objet de l'interconnexion.

(3) L'interconnexion n'est autorisée que dans le respect des finalités identiques ou liées de fichiers et du secret professionnel auquel les responsables du traitement sont le cas échéant astreints.

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

(1) Font l'objet d'un règlement grand-ducal :

- (a) les traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions pénales qui sont réservés, conformément à leurs missions légales et réglementaires respectives, aux organes du corps de la police grand-ducale, de l'Inspection générale de la police et de l'administration des douanes et accises. Le règlement grand-ducal déterminera le responsable du traitement, la condition de légitimité du traitement, la ou les finalités du traitement, la ou les catégories de personnes concernées et les données ou les catégories de données s'y rapportant, l'origine de ces données, les tiers ou les catégories de tiers auxquels ces données peuvent être communiquées et les mesures à prendre pour assurer la sécurité du traitement en application de l'article 22 de la présente loi,
- (b) les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique, et
- (c) les traitements de données dans des domaines du droit pénal effectués en vertu de conventions internationales, d'accords intergouvernementaux ou dans le cadre de la coopération avec l'Organisation internationale de police criminelle (OIPC – Interpol).

(2) Le contrôle et la surveillance des traitements mis en œuvre tant en application d'une disposition de droit interne qu'en application d'une convention internationale est exercé par une autorité de contrôle composée du Procureur Général d'Etat, ou de son délégué qui la préside, et de deux membres de la Commission nationale nommés, sur proposition de celle-ci, par le ministre.

L'organisation et le fonctionnement de l'autorité de contrôle font l'objet d'un règlement grand-ducal.

L'autorité de contrôle est informée immédiatement de la mise en œuvre d'un traitement de données visé par le présent article. Elle veille à ce que ces traitements soient effectués conformément aux dispositions légales qui les régissent.

Pour l'exercice de sa mission, l'autorité de contrôle a un accès direct aux données traitées. Elle peut procéder, quant aux traitements effectués, à des vérifications sur place et se faire communiquer tous renseignements et documents utiles à sa mission. Elle peut également charger un de ses membres à procéder à des missions de contrôle spécifique qui sont exécutées dans les conditions indiquées ci-dessus.

L'autorité de contrôle fait opérer les rectifications et radiations nécessaires.

Elle présente chaque année au ministre un rapport rendant compte de l'exécution de sa mission.

Le droit d'accès aux données visées au présent article ne peut être exercé que par l'intermédiaire de l'autorité de contrôle. Celle-ci procède aux vérifications et investigations utiles, fait opérer les rectifications nécessaires et informe la personne concernée que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exécution.

(3) Toute personne, agissant à titre privé, qui effectue un traitement en violation des dispositions du présent article est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

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

### **Art. 18. – Principes**

(1) Le transfert vers un pays tiers de données faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat et moyennant le respect des dispositions de la présente loi et de ses règlements d'exécution.

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

(3) En cas de doute, le responsable du traitement informe sans délai la Commission nationale qui apprécie si un pays tiers assure un niveau de protection adéquat. La Commission nationale notifie conformément à l'article 20 à la Commission européenne les cas dans lesquels elle estime que le pays tiers n'assure pas un niveau de protection adéquat.

(4) Lorsque la Commission européenne ou la Commission nationale constate qu'un pays tiers ne dispose pas d'un niveau de protection adéquat, tout transfert de données vers ce pays est prohibé.

(5) Quiconque effectue un transfert de données vers un pays tiers en violation des dispositions des paragraphes (1), (2) et (4) qui précèdent est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du transfert contraire aux dispositions des paragraphes (1), (2) et (4) du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

### **Art. 19. – Dérogations**

(1) Le transfert de données ou d'une catégorie de données vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 18, paragraphe (2), peut toutefois être effectué à condition que:

- (a) la personne concernée ait donné son consentement au transfert envisagé, ou
- (b) le transfert soit nécessaire à l'exécution d'un contrat auquel la personne concernée et le responsable du traitement sont parties ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée, ou
- (c) le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers, ou
- (d) le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice, ou
- (e) le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou
- (f) le transfert intervienne depuis un registre public tel que prévu à l'article 12, paragraphe (3) lettre (b).

(2) Dans le cas d'un transfert effectué vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 18, paragraphe (2), le responsable du traitement doit notifier à la Commission nationale un rapport établissant les conditions dans lesquelles il a opéré le transfert.

(3) Sans préjudice des dispositions du paragraphe (1), la Commission nationale peut autoriser, sur la base d'une demande dûment motivée, un transfert ou un ensemble de transferts de données vers un pays tiers et n'assurant pas un niveau de protection adéquat, au sens de l'article 18, paragraphe (2), ceci lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes concernées, ainsi qu'à l'exercice des droits correspondants. Ces garanties peuvent résulter de clauses contractuelles appropriées. Le responsable du traitement est tenu de se conformer à la décision de la Commission nationale.

(4) Quiconque effectue un transfert de données vers un pays tiers en violation des dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du transfert contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

**Art. 20. – Information réciproque**

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

(2) Le ministre informe la Commission nationale de toute décision relative au niveau de protection d'un pays tiers prise par la Commission européenne.

**Chapitre V. – Subordination et sécurité des traitements**

**Art. 21. – Subordination**

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

**Art. 22. – Sécurité des traitements**

(1) Le responsable du traitement doit mettre en œuvre toutes les mesures techniques et d'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illícite, 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 illícite. Ces mesures font l'objet d'un rapport annuel à soumettre par le responsable du traitement à la Commission nationale.

(2) Lorsque le traitement est mis en œuvre pour compte du responsable du traitement, celui-ci doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect de ces mesures.

(3) Tout traitement effectué pour compte doit être régi par un contrat ou un acte juridique congné par écrit qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que:

- (a) le sous-traitant n'agit que sur la seule instruction du responsable du traitement; et que
- (b) les obligations visées au présent article incombent également à celui-ci.

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

En fonction du risque d'atteinte à la vie privée, ainsi que de l'état de l'art et des coûts liés à leur mise en œuvre, les mesures visées à l'article 22, paragraphe (1) doivent:

- (a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données (contrôle à l'entrée des installations);
- (b) empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée (contrôle des supports);
- (c) empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées (contrôle de la mémoire);
- (d) empêcher que des systèmes de traitements de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation);
- (e) garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur compétence (contrôle de l'accès);

- (f) garantir que puisse être vérifié et constaté l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission (contrôle de la transmission);
- (g) garantir que puisse être vérifié et constaté a posteriori l'identité des personnes ayant eu accès au système d'information et quelles données ont été introduites dans le système, à quel moment et par quelle personne (contrôle de l'introduction);
- (h) empêcher que, lors de la communication de données et du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport);
- (i) sauvegarder les données par la constitution de copies de sécurité (contrôle de la disponibilité).

**Art. 24. – Secret professionnel**

(1) Les membres de la Commission nationale et toute personne qui exerce des fonctions auprès de la Commission nationale ou accomplit une mission pour son compte ainsi que le chargé de la protection des données sont soumis au respect du secret professionnel prévu à l'article 458 du Code pénal, même après la fin de leur fonction.

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

(3) Le prestataire de service de certification ne peut opposer à la Commission nationale le secret professionnel auquel il est soumis conformément à l'article 19 de la loi du 14 août 2000 relative au commerce électronique.

(4) Le responsable du traitement agissant dans le cadre de l'accomplissement de ses missions visées à l'article 7, paragraphe (1), ne peut opposer à la Commission nationale le secret professionnel auquel il est soumis lorsque celle-ci a été saisie conformément à l'article 32, paragraphes (4) et (5).

**Art. 25. – Sanctions relatives à la subordination et à la sécurité des traitements**

Quiconque effectue un traitement en violation des règles relatives à la confidentialité ou à la sécurité visées aux articles 21, 22 et 23 est puni d'un emprisonnement de huit jours à six mois et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions des articles 21, 22 et 23 sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

**Chapitre VI. – Droits de la personne concernée**

**Art. 26. – Le droit à l'information de la personne concernée**

(1) Lorsque des données sont collectées directement auprès de la personne concernée, le responsable du traitement doit fournir à la personne concernée, au plus tard lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes, sauf si la personne concernée en a déjà été informée:

- (a) l'identité du responsable du traitement et, le cas échéant, de son représentant;
- (b) la ou les finalités déterminées du traitement auquel les données sont destinées;
- (c) toute autre information supplémentaire telle que:
  - les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
  - le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse;
  - l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;
  - la durée de conservation des données.

(2) Lorsque les données n'ont pas été collectées auprès de la personne concernée, le responsable du traitement doit, dès l'enregistrement des données ou, si une communication de données à un tiers est

envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée, sauf si elle en est déjà informée, les informations suivantes:

- (a) l'identité du responsable du traitement et, le cas échéant, de son représentant;
- (b) la ou les finalités déterminées du traitement auquel les données sont destinées;
- (c) toute information supplémentaire telle que:
  - les catégories de données concernées;
  - les destinataires ou les catégories de destinataires des données auxquels les données sont susceptibles d'être communiquées;
  - l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;
  - la durée de conservation des données.

(3) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

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

(1) L'article 26, paragraphes (1) et (2), ne s'applique pas lorsque le traitement est nécessaire pour sauvegarder:

- (a) la sûreté de l'Etat;
- (b) la défense;
- (c) la sécurité publique;
- (d) la prévention, la recherche, la constatation et la poursuite d'infractions pénales y compris celles à la lutte contre le blanchiment, ou le déroulement de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi;
- (e) un intérêt économique ou financier important de l'Etat ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;
- (f) la protection de la personne concernée ou des droits et libertés d'autrui,

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

(3) Les dispositions de l'article 26 paragraphes (1) et (2) ne s'appliquent pas lorsque, en particulier pour un traitement ayant une finalité statistique, historique ou scientifique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si l'enregistrement ou la communication des données est prévu par la loi.

(4) Quiconque contrevient aux dispositions des paragraphes (1) et (2) qui précèdent est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions des paragraphes (1) et (2) du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

**Art. 28. – Droit d'accès**

(1) Sur demande à introduire auprès du responsable du traitement, la personne concernée ou ses ayants droit justifiant d'un intérêt légitime peuvent obtenir sans frais, à des intervalles raisonnables et sans délais excessifs:

- (a) l'accès aux données la concernant;
- (b) la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, sur les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées;

- (c) la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données;
- (d) la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 31.

(2) Celui qui entrave sciemment par quelque moyen que ce soit, l'exercice du droit d'accès, sera puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article.

(3) Le patient a un droit d'accès aux données le concernant. Le droit d'accès est exercé par le patient lui-même ou par l'intermédiaire d'un médecin qu'il désigne.

En cas de décès du patient, son conjoint non séparé de corps et ses enfants ainsi que toute personne qui au moment du décès a vécu avec lui dans le ménage ou, s'il s'agit d'un mineur, ses père et mère, peuvent exercer, par l'intermédiaire d'un médecin qu'ils désignent, le droit d'accès dont question à l'alinéa qui précède.

Le droit d'accès du patient pourra encore être exercé, du vivant d'une personne placée sous le régime de la curatelle ou sous celui de la tutelle tel qu'il est organisé par la loi du 11 août 1982, par l'intermédiaire d'un médecin désigné par son curateur ou tuteur.

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

(5) Selon le cas, le responsable du traitement procédera à la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente loi, notamment en raison du caractère incomplet ou inexact des données, sous peine d'encourir dans les conditions de l'article 33 l'interdiction temporaire ou définitive du traitement ou la destruction des données.

(6) Toute personne qui dans l'exercice de son droit d'accès a des raisons sérieuses d'admettre que les données qui lui ont été communiquées ne sont pas conformes aux données traitées, peut en informer la Commission nationale qui procède aux vérifications nécessaires.

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

(8) Sans préjudice de la sanction prévue au paragraphe (5), quiconque contrevient sciemment aux dispositions du présent article ou quiconque prend sciemment un nom ou prénom supposé ou une fausse qualité pour obtenir communication des données faisant l'objet d'un traitement en application du paragraphe (1), est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article.

#### **Art. 29. – Exceptions au droit d'accès**

(1) Le responsable du traitement peut limiter ou différer l'exercice du droit d'accès d'une personne concernée lorsqu'une telle mesure est nécessaire pour sauvegarder:

- (a) la sûreté de l'Etat;
- (b) la défense;
- (c) la sécurité publique;
- (d) la prévention, la recherche, la constatation et la poursuite d'infractions pénales y compris celles à la lutte contre le blanchiment, ou le déroulement de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi;

- (e) un intérêt économique ou financier important de l'Etat ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;
- (f) la protection de la personne concernée ou des droits et libertés d'autrui;
- (g) la liberté d'expression et que la mesure d'exception est prise conformément à l'article 28, paragraphe (4);
- (h) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points (c), (d) et (e).

(2) Au cas où il n'existe manifestement aucun risque d'atteinte à la vie privée d'une personne concernée, le responsable du traitement peut limiter le droit d'accès lorsque les données sont traitées exclusivement aux fins de recherche scientifique ou sont stockées sous la forme de données pendant une durée n'excédant pas celle nécessaire à la seule finalité d'établissement de statistiques et que ces données ne puissent être utilisées aux fins de prendre une mesure ou une décision se rapportant à des personnes précises.

(3) Le responsable du traitement doit indiquer le motif pour lequel il limite ou diffère l'exercice du droit d'accès. Lorsque le droit d'accès est différé, le responsable du traitement doit indiquer la date à partir de laquelle le droit d'accès peut à nouveau être exercé. Le responsable du traitement notifiera le motif à la Commission nationale.

(4) En cas de limitation de l'exercice du droit d'accès de la personne concernée, le droit d'accès est exercé par la Commission nationale qui dispose d'un pouvoir d'investigation en la matière et qui fait opérer la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente loi. La Commission nationale peut communiquer à la personne concernée le résultat de ses investigations, sans toutefois mettre en danger la ou les finalités des traitements en question.

(5) Quiconque contrevient à la disposition du paragraphe (3) qui précède est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du paragraphe (3) du présent article.

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

(1) Toute personne concernée a le droit:

- (a) de s'opposer à tout moment pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de dispositions légales prévoyant expressément le traitement. En cas d'opposition justifiée, le traitement mis en oeuvre par le responsable du traitement ne peut pas porter sur ces données;
- (b) de s'opposer, sur demande et gratuitement, au traitement la concernant envisagé par le responsable du traitement à des fins de prospection; il incombe au responsable du traitement de porter l'existence de ce droit à la connaissance de la personne concernée;
- (c) d'être informée avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

(2) Quiconque contrevient sciemment aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article.

### **Art. 31. – Décisions individuelles automatisées**

Une personne peut être soumise à une décision individuelle automatisée produisant des effets juridiques à son égard, si cette décision:

- (a) est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telle que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime, ou

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

## **Chapitre VII. – Contrôle et surveillance de l'application de la loi**

### **Art. 32. – Missions et pouvoirs de la Commission nationale**

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

(2) Tous les ans, la Commission nationale rend compte, dans son rapport écrit aux membres du Gouvernement en conseil, de l'exécution de ses missions. Dans ce rapport, elle relève plus particulièrement l'état des notifications et des autorisations, les déficiences ou abus qui ne sont pas spécifiquement visés par les dispositions légales, réglementaires et administratives existantes. Elle publiera son rapport annuel.

Le rapport est avisé par la commission consultative des droits de l'homme, organe consultatif du gouvernement en matière de droits de l'homme sur le territoire du Grand-Duché de Luxembourg dont la composition et les attributions sont déterminées par règlement grand-ducal.

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

- (a) assurer l'application des dispositions de la présente loi et de ses règlements d'exécution en particulier celles relatives à la confidentialité et à la sécurité des traitements;
- (b) recevoir les notifications préalables à la mise en oeuvre d'un traitement, de même que les changements affectant le contenu de ces notifications, et procéder a posteriori au contrôle de la licéité des traitements notifiés; de même elle est informée sans délai de tout traitement soumis à autorisation préalable;
- (c) assurer la publicité des traitements lui notifiés en tenant un registre afférent, sauf disposition contraire;
- (d) autoriser la mise en oeuvre des traitements soumis au régime de l'article 14 de la présente loi;
- (e) être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi. Ces avis sont publiés au rapport annuel visé à l'article 15, paragraphe (6);
- (f) présenter au Gouvernement toutes suggestions susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données;
- (g) recevoir et le cas échéant après discussion avec les auteurs approuver les codes de conduite relatifs à un traitement ou un ensemble de traitements lui soumis par des associations professionnelles représentatives de responsables du traitement;
- (h) conseiller le Gouvernement, soit à la demande de celui-ci, soit sur sa propre initiative, au sujet des conséquences de l'évolution des technologies de traitement de l'information au regard du respect des libertés et droits fondamentaux des personnes; à cette fin, elle peut faire procéder à des études, des enquêtes ou expertises;
- (i) favoriser de façon régulière et par tout moyen qu'elle juge opportun, la diffusion d'informations relatives aux droits des personnes concernées et aux obligations des responsables du traitement, notamment en ce qui concerne le transfert de données vers des pays tiers.

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

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

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

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

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

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

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

(11) Quiconque empêche ou entrave sciemment, de quelque manière que ce soit, l'accomplissement des missions incombant à la Commission nationale, est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. Est considéré comme empêchant ou entravant sciemment l'accomplissement des missions incombant à la Commission nationale, le refus opposé à ses membres de donner accès aux locaux autres que les locaux d'habitation, où a lieu un traitement aux données faisant l'objet d'un traitement ou de communiquer tous renseignements et documents demandés. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article.

### **Art. 33. – Sanctions administratives**

(1) La Commission nationale peut prendre les sanctions disciplinaires suivantes:

- (a) avertir ou admonester le responsable du traitement ayant violé les obligations lui imposées par les articles 21 à 24;
- (b) verrouiller, effacer ou détruire des données faisant l'objet d'un traitement contraire aux dispositions de la présente loi ou de ses règlements d'exécution;
- (c) interdire temporairement ou définitivement un traitement contraire aux dispositions de la présente loi ou à ses règlements d'exécution;
- (d) ordonner l'insertion intégrale ou par extraits de la décision d'interdiction par la voie des journaux ou de toute autre manière, aux frais de la personne sanctionnée.

(2) Les décisions ci-dessus sont susceptibles d'un recours en réformation suivant l'article 3 de la loi du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif.

### **Art. 34. – Composition de la Commission nationale**

(1) La Commission nationale est une autorité publique qui prend la forme d'un établissement public. Son siège est fixé à Luxembourg-ville. Il peut être transféré à tout moment dans toute autre localité du Luxembourg par voie de règlement grand-ducal.

La Commission nationale dispose de la personnalité juridique et jouit de l'autonomie financière et administrative, sous la tutelle du ministre.

Elle exerce en toute indépendance les missions dont elle est investie en vertu de la présente loi.

(2) La Commission nationale est composée de trois membres effectifs et de trois membres suppléants nommés et révoqués par le Grand-Duc sur proposition du Gouvernement en conseil. Le président est désigné par le Grand-Duc. Les membres sont nommés pour un terme de six ans, renouvelable une fois.

Le Gouvernement en conseil propose au Grand-Duc comme membre effectif et suppléant chaque fois au moins un juriste et un informaticien justifiant d'une formation universitaire accomplie.

Avant d'entrer en fonction, le président de la Commission nationale prête entre les mains du Grand-Duc ou de son représentant le serment suivant: „Je jure fidélité au Grand-Duc, obéissance à la constitution et aux lois de l'Etat. Je promets de remplir mes fonctions avec intégrité, exactitude et impartialité.“

Avant d'entrer en fonction, les membres de la Commission nationale prêtent entre les mains du président de la Commission nationale le serment suivant: „Je jure fidélité au Grand-Duc, obéissance à la constitution et aux lois de l'Etat. Je promets de remplir mes fonctions avec intégrité, exactitude et impartialité.“

Lorsque le président ou un membre effectif de la Commission nationale est issu du secteur public, il obtient un congé spécial pour la durée de son mandat avec maintien de tous les avantages et droits découlant de son statut respectif. Il continue notamment à jouir de son traitement, indemnité ou salaire suivant le cas, ainsi que du régime de sécurité sociale correspondant à son statut.

En cas de cessation du mandat, il est réintégré sur sa demande dans son administration d'origine à un emploi correspondant au traitement qu'il a touché précédemment, augmenté des échelons et majorations de l'indice se rapportant aux années de service passées comme président ou membre effectif jusqu'à concurrence du dernier échelon du grade.

A défaut de vacance, il peut être créé un emploi hors cadre correspondant à ce traitement; cet emploi est supprimé de plein droit à la première vacance qui se produit dans une fonction appropriée du cadre normal.

Lorsque le président ou un membre effectif de la Commission nationale est issu du secteur privé, il touche une rémunération calculée par référence à la réglementation fixant le régime des indemnités des employés occupés dans les administrations et services de l'Etat qui est applicable en la matière, sur base d'une décision individuelle prise en vertu de l'article 23 du règlement grand-ducal du 28 juillet 2000 fixant le régime des indemnités des employés occupés dans les administrations et services de l'Etat.

Il reste affilié au régime de sécurité sociale auquel il était soumis pendant l'exercice de sa dernière occupation.

En cas de cessation du mandat, il touche pendant une durée maximale d'un an une indemnité d'attente mensuelle correspondant au salaire ou traitement mensuel moyen du dernier revenu professionnel cotisable annuel mis en compte au titre de sa carrière d'assurance en cours avant le début de sa fonction de président ou de membre effectif de la Commission nationale.

Cette indemnité d'attente est réduite dans la mesure où l'intéressé touche un revenu professionnel ou bénéficie d'une pension personnelle.

Le président et les membres effectifs de la Commission nationale bénéficient d'une indemnité spéciale tenant compte de l'engagement requis par les fonctions, à fixer par règlement grand-ducal.

La démission d'un membre de la Commission nationale intervient de plein droit par l'atteinte de la limite d'âge de 65 ans.

Les membres suppléants touchent une indemnité dont le montant est fixé par règlement grand-ducal.

(3) Les membres de la Commission nationale ne peuvent être membre du Gouvernement, de la Chambre des Députés, du Conseil d'Etat ou du Parlement Européen ni exercer d'activité professionnelle ou détenir directement ou indirectement des intérêts dans une entreprise ou tout autre organisme opérant dans le champ des traitements de données.

(4) Si, en cours de mandat un membre de la Commission nationale cesse d'exercer ses fonctions, le mandat de son successeur est limité à la période restant à courir.

### **Art. 35. – *Fonctionnement de la Commission nationale***

(1) La Commission nationale est un organe collégial. Elle établit son règlement intérieur comprenant ses procédures et méthodes de travail dans le mois de son installation. Le règlement intérieur est publié au Mémorial.

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

(a) les règles de procédure applicables devant la Commission nationale,

- (b) les conditions de fonctionnement de la Commission nationale,
- (c) l'organisation des services de la Commission nationale.

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

Les membres effectifs empêchés d'assister à une réunion sont tenus d'en avertir leur suppléant et de lui continuer la convocation.

(4) La Commission nationale ne peut valablement siéger ni délibérer qu'à condition de réunir trois membres.

(5) Les membres de la Commission nationale ne peuvent siéger, délibérer ou décider dans aucune affaire dans laquelle ils ont un intérêt direct ou indirect.

(6) Les délibérations sont prises à la majorité des voix. Les abstentions ne sont pas recevables.

(7) Le Gouvernement en conseil ayant proposé à la nomination un membre de la Commission nationale peut proposer sa révocation au Grand-Duc. La Commission nationale est entendue en son avis avant toute révocation.

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

**Art. 36. – Statut des membres et agents de la Commission nationale**

(1) Le cadre du personnel de la Commission nationale comprend les fonctions et emplois suivants:

Dans la carrière moyenne de l'administration, grade de computation de la bonification d'ancienneté: grade 7, carrière du rédacteur:

- des inspecteurs principaux 1er en rang
- des inspecteurs principaux
- des inspecteurs
- des chefs de bureau
- des chefs de bureau adjoints
- des rédacteurs principaux
- des rédacteurs

Les agents de la carrière moyenne des rédacteurs sont des fonctionnaires de l'Etat en ce qui concerne notamment leur statut, leur traitement et leur régime de pension qui est régi par les dispositions légales régissant les fonctionnaires de l'Etat.

(2) Le cadre prévu au paragraphe (1) ci-dessus peut être complété par des employés de l'Etat ainsi que par des ouvriers de l'Etat dans les limites des crédits disponibles. La rémunération des employés de l'Etat est fixée conformément au règlement grand-ducal du 28 juillet 2000 fixant le régime des indemnités des employés occupés dans les administrations et services de l'Etat.

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

(4) La Commission nationale peut, dans des cas déterminés, faire appel à des experts externes dont les prestations sont définies et rémunérées sur la base d'un contrat de droit privé.

**Art. 37. – Dispositions financières**

(1) Au moment de sa création, la Commission nationale bénéficie d'une dotation initiale de deux cent mille euros à charge du budget de l'Etat. L'Etat met à sa disposition les biens mobiliers et immobiliers nécessaires au bon fonctionnement et à l'exercice de ses missions.

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

(3) Avant le 31 mars de chaque année, la Commission nationale arrête son compte d'exploitation de l'exercice précédent, ensemble avec son rapport de gestion. Avant le 30 septembre de chaque exercice, la Commission nationale arrête le budget pour l'exercice à venir. Le budget, les comptes annuels et les rapports arrêtés sont transmis au Gouvernement en conseil qui décide de la décharge à donner à la Commission nationale. La décision constatant la décharge accordée à la Commission nationale ainsi que les comptes annuels de la Commission nationale sont publiés au Mémorial.

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

(5) La loi du 27 novembre 2001 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2002 est modifiée comme suit: il est ajouté au budget des dépenses au Chapitre III – Dépenses courantes sous „00 – Ministère d'Etat“ une section „00.9 Commission nationale pour la protection des données“ émargeant les articles suivants:

„12.300: Prise en charge par l'Etat des frais encourus par la Commission nationale pour la protection des données. (crédit non limitatif et sans distinction d'exercice) .....	200.870
33.000: Dotation initiale en faveur de la Commission nationale pour la protection des données .....	200.000“

### **Chapitre VIII. – Recours juridictionnels**

#### **Art. 38. – Généralités**

Sans préjudice des sanctions pénales instituées par la présente loi et des actions en responsabilité régies par le droit commun, en cas de mise en œuvre d'un traitement en violation des formalités prévues par la présente loi toute personne dispose d'un recours juridictionnel tel que prévu ci-après.

#### **Art. 39. – Action en cessation**

(1) A la requête

- du Procureur d'Etat qui a déclenché une action publique pour violation de la présente loi,
- de la Commission nationale, dans l'hypothèse où une sanction disciplinaire visée à l'article 33 de la présente loi, qui n'a pas fait l'objet d'un recours ou qui a été confirmée par la juridiction administrative, n'a pas été respectée, ou
- d'une personne lésée, dans l'hypothèse où la Commission nationale n'a pas pris position sur une saisine intervenue sur la base de l'article 32, paragraphe (4), (5) ou (6) de la présente loi,

le président du tribunal d'arrondissement du lieu où le traitement est mis en œuvre, ou le juge qui le remplace, ordonne la cessation du traitement contraire aux dispositions de la présente loi et la suspension provisoire de l'activité du responsable du traitement ou du sous-traitant. Le président du tribunal d'arrondissement, ou le juge qui le remplace, peut ordonner la fermeture provisoire de l'établissement du responsable du traitement ou du sous-traitant lorsque sa seule activité est de traiter des données.

(2) L'action est recevable même lorsque le traitement illégal a pris fin ou n'est plus susceptible de se reproduire.

(3) L'action est introduite et jugée comme en matière de référé conformément aux articles 932 à 940 du Nouveau code de procédure civile. Toutefois, par dérogation à l'article 939, alinéa 2, du Nouveau code de procédure civile, l'ordonnance de référé n'est pas susceptible d'opposition.

(4) Sont également applicables les articles 2059 à 2066 du Code civil.

(5) La publication de la décision peut être ordonnée, en totalité ou par extrait, aux frais du contrevenant, par la voie des journaux ou de toute autre manière. Il ne peut être procédé à la publication qu'en vertu d'une décision judiciaire coulée en force de chose jugée.

(6) La suspension provisoire et le cas échéant la fermeture provisoire peuvent être ordonnées indépendamment de l'action publique. La suspension provisoire ou la fermeture provisoire ordonnée par le président du tribunal d'arrondissement, ou par le juge qui le remplace, prend toutefois fin en cas de décision de non-lieu ou d'acquittement, et au plus tard à l'expiration d'un délai de deux ans à partir de la décision initiale de suspension ou de fermeture.

### **Chapitre IX. – Le chargé de la protection des données**

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

(1) Tout responsable de traitement peut, dans le cadre de l'article 12, paragraphe (3) sous (a), et aux fins y visées, désigner un chargé de la protection des données, dont il communique l'identité à la Commission nationale.

(2) Les pouvoirs du chargé de la protection des données sont les suivants:

- (a) un pouvoir d'investigation aux fins d'assurer la surveillance du respect des dispositions de la présente loi et de ses règlements d'exécution par le responsable du traitement;
- (b) un droit d'information auprès du responsable du traitement et corrélativement, un droit d'informer le responsable du traitement des formalités à accomplir afin de se conformer aux dispositions de la présente loi et de ses règlements d'exécution.

(3) Dans l'exercice de ses missions le chargé de la protection des données est indépendant vis-à-vis du responsable du traitement qui le désigne:

- (a) il ne connaît aucun lien de subordination vis-à-vis du responsable du traitement et ne peut être lié au responsable du traitement par un contrat de travail;
- (b) il ne peut être révoqué pour des raisons liées à l'exercice de ses missions, hormis le cas de la violation de ses obligations légales ou conventionnelles.

(4) Le chargé de la protection consulte la Commission nationale en cas de doute quant à la conformité à la présente loi d'un traitement mis en œuvre sous sa surveillance.

(5) Peuvent être désignés à la fonction de chargé de la protection des données les personnes physiques et morales qui sont agréées par la Commission nationale.

(6) L'agrément pour l'activité du chargé de la protection des données est subordonné à la justification d'une formation universitaire accomplie en droit, économie, gestion d'entreprise, sciences de la nature, ou informatique ainsi que d'assises financières d'une valeur de 20.000 euros.

(7) Par dérogation au paragraphe précédent, les membres inscrits dans une des professions réglementées suivantes peuvent être agréés comme chargé de la protection des données sans autre condition: avocat à la Cour, réviseur d'entreprises, expert-comptable, médecin.

Un règlement grand-ducal peut ajouter à cette liste d'autres professions réglementées et assujetties à un organisme de surveillance ou de discipline, soit officiel soit propre à la profession et reconnu par la loi.

(8) La Commission nationale vérifie les qualités de tout chargé de la protection des données.

Elle peut s'opposer à tout moment à la désignation ou au maintien du chargé de la protection des données lorsqu'il:

- (a) ne présente pas les qualités requises pour la fonction de chargé de la protection des données; ou
- (b) est d'ores et déjà en relation avec le responsable du traitement dans le cadre d'autres activités que celle du traitement des données et que cette relation fait naître un conflit d'intérêts limitant son indépendance.

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

(9) La Commission nationale définit les modalités du contrôle continu des qualités requises à la fonction de chargé de la protection des données.

(10) Un règlement grand-ducal fixera les modalités de désignation et de révocation du chargé de protection des données, d'exécution de ses missions, de même que ses relations avec la Commission nationale.

### **Chapitre X. – Dispositions spécifiques, transitoires et finales**

#### **Art. 41. – Dispositions spécifiques**

- (1) (a) Les autorités compétentes visées aux articles 88-1 à 88-4 du Code d'instruction criminelle, et  
 (b) les autorités agissant dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du Code d'instruction criminelle,

accèdent de plein droit, sur requête et par l'intermédiaire de l'Institut luxembourgeois de régulation (ci-après „ILR“) aux données concernant l'identité des abonnés et utilisateurs des opérateurs et fournisseurs de communications électroniques ainsi que des services postaux et des fournisseurs de ces services.

La centrale des secours d'urgence 112 et la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg accèdent dans les mêmes conditions et modalités que les autorités visées à l'alinéa précédent aux seules données concernant l'identité des abonnés et utilisateurs des opérateurs et fournisseurs de communications électroniques.

(2) A ces fins, les opérateurs et les fournisseurs mettent d'office et gratuitement à la disposition de l'ILR les données prescrites au paragraphe (1). Les données doivent être actualisées au moins une fois par jour. L'accès doit être garanti vingt-quatre heures sur vingt-quatre et sept jours sur sept. Un règlement grand-ducal détermine les services de communications électroniques et services postaux pour lesquels les opérateurs et fournisseurs de services doivent mettre à disposition les données ainsi que la nature, le format et les modalités de mise à disposition des données.

(3) L'accès de plein droit se limite aux mesures spéciales de surveillance telles que prévues aux articles 88-1 à 88-4 du Code d'instruction criminelle, celles prises en matière de crime flagrant ou dans le cadre de l'article 40 du Code d'Instruction criminelle et aux mesures particulières de secours d'urgence prestées dans le cadre des activités de la centrale des secours d'urgence 112 et de la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg.

(4) La procédure est entièrement automatisée suite à l'autorisation de la Commission nationale. La Commission nationale vérifiera en particulier la sécurisation du système informatique utilisé. Cette automatisation permettra l'accès à distance par voie de communication électronique.

#### **Art. 42. – Dispositions transitoires**

(1) Les traitements existant dans des fichiers non automatisés ou automatisés antérieurs à l'entrée en vigueur de la présente loi doivent être rendus conformes aux dispositions du chapitre II et du chapitre VI, dans un délai de deux ans à compter de la date d'entrée en vigueur de la présente loi.

(2) Toutefois la personne concernée peut obtenir, sur demande, et notamment en ce qui concerne l'exercice de son droit d'accès, la rectification, l'effacement ou le verrouillage des données incomplètes, inexactes ou conservées de manière incompatible aux fins légitimes poursuivies par le responsable du traitement.

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

#### **Art. 43. – Mise en vigueur des dispositions transitoires**

(1) La Commission nationale établira le schéma de notification prévu à l'article 13, paragraphe (3), dans les quatre mois de la nomination de ses membres. Elle informera le public, moyennant publication au Mémorial et communiqué de presse aux journaux édités au Luxembourg, de la date à partir de laquelle le schéma de notification est disponible auprès de la Commission nationale.

(2) Les responsables du traitement procéderont à la notification de leurs traitements dans les quatre mois à partir de la date de la publication officielle mentionnée au paragraphe (1).

(3) Les responsables du traitement dont les traitements sont autorisés, lors de l'entrée en vigueur de la présente loi, moyennant règlement grand-ducal ou arrêté ministériel „autorisant la création et l'exploitation d'une banque de données“, ne notifieront ou ne demanderont l'autorisation de leurs traitements qu'à l'expiration de la durée de validité de l'autorisation octroyée, à moins que pour des raisons de conformité avec les dispositions de la présente loi, ils jugent nécessaire de le faire auparavant.

(4) Les traitements non automatisés de données contenues ou appelées à figurer dans un fichier sont à notifier dans les douze mois à partir de la date de la publication officielle mentionnée au paragraphe (1).

**Art. 44. – Dispositions finales**

(1) La loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques est abrogée.

(2) Pour autant qu'ils ne sont pas contraires aux dispositions de la présente loi, les règlements pris en exécution de la loi modifiée du 31 mars 1979 précitée resteront en vigueur tant qu'ils n'auront pas été remplacés par de nouvelles dispositions.

**Art. 45. – Entrée en vigueur**

La présente loi entre en vigueur le premier jour du quatrième mois qui suit sa publication au Mémorial. Par dérogation à ce qui précède, les articles 34, 35, 36 et 37 entrent en vigueur trois jours après publication de la présente loi au Mémorial.

Luxembourg, le 10 juillet 2002

*Le Président,*  
Laurent MOSAR

*Le Rapporteur,*  
Patrick SANTER

