LA LOI DU 2 AOÛT 2002 SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL : UNE NOUVELLE DONNÉE POUR LA PLACE FINANCIÈRE

Patrick Santer
Avocat à la Cour
Elvinger, Hoss & Prussen

Toinon Hoss
Avocat à la Cour
Elvinger, Hoss & Prussen

13-1. L'adoption de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après, la « loi »), entrée en vigueur le 1er décembre 2002, est presque passée inaperçue, peut-être en raison de son caractère technique rendant difficile toute tentative de vulgarisation. On peut le regretter, car cette loi devrait bouleverser les habitudes tant des personnes qui traitent des données à caractère personnel que de celles dont les données sont traitées.

La loi du 31 mars 1979, qui se trouve abrogée par la loi, ne répondait plus aux impératifs d'une société de l'information digne de ce nom. À l'époque, le Luxembourg s'était rangé parmi les premiers à se doter d'une législation en matière de protection des données[1], après le Land de Hesse (1970), la Suède (1973), la RFA et le Canada (1977), la France, la Norvège, le Danemark et

[1] Les termes « protection des données » constituent un usage linguistique inexact dans la mesure où le but poursuivi n'est pas de protéger des données mais de protéger les personnes dont les données à caractère personnel font l'objet d'un traitement contre tout abus (voy. *Doc. parl.* 4735, p. 79 ; *Doc. parl.* 4735-13, p. 6). La présente analyse utilisera néanmoins ces termes qui sont entrés dans le langage courant.

l'Autriche (1978). Si le but de la loi de 1979, à savoir la protection des personnes physiques et morales contre une utilisation abusive de données nominatives[2] restait inchangé, l'évolution technologique qui a marqué ces vingt dernières années a rendu l'application de cette loi « illusoire »[3]. En effet, la loi de 1979 soumettait toute banque de données, c'est-à-dire tout lieu où sont stockées des données nominatives, à une autorisation ministérielle préalable, après avis d'une commission consultative.

13-2. L'omniprésence et la démocratisation de l'outil informatique ont rendu impossible le respect de cette loi et il fallait être idéaliste ne serait-ce que pour tenter de s'y conformer. La loi du 31 mars 1979 était ainsi tombée en désuétude.

L'obligation de transposer la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[4] a fourni au législateur luxembourgeois l'occasion de réformer de fond en comble les règles gouvernant la protection des données[5].

Le but recherché tant par le législateur luxembourgeois que par la Communauté européenne est de concilier le respect des droits et libertés fondamentaux des citoyens[6], et notamment le respect dû à la vie privée, avec les impératifs de la société de l'information. Il faut que les données puissent circuler librement au sein de la Communauté européenne entre les acteurs de la vie économique, sociale et scientifique, que ces acteurs soient publics ou privés, sans compter le nombre croissant de données à caractère personnel échangées entre administrations publiques[7]. « Bien qu'il soit conçu pour protéger les personnes, l'objectif de ce régime n'est pas de réduire la circulation des données. Il s'agit plutôt d'en réglementer la circulation de manière à atteindre un équilibre acceptable entre la protection de la sphère privée de l'individu et les intérêts que réclament au contraire une circulation et une utilisation plus large de l'information »[8]. Déjà, l'intitulé de la directive 95/46/CE « relative à la protection des personnes physiques à l'égard du traitement des donnés à caractère personnel et à la libre circulation de ces données » est révélateur à cet égard.

[2] Art. 1er de la loi du 31 mars 1979 (*Mémorial* A, 1992, p. 2242).

[3] *Doc. parl.* 4735-13, p. 3.

[4] *J.O.C.E.* L 281/1995, p. 31. Le texte de la directive est publié au *Document parlementaire* 4735 aux pages 53 et suivantes.

[5] Le Luxembourg a été condamné par la C.J.C.E. le 4 octobre 2001 pour non-transposition de la directive 95/46/CE (aff. C-450/00) .

[6] Encore qu'il peut sembler que le législateur est allé plus loin en incluant les personnes morales dans le cercle des personnes « protégées ».

[7] À titre d'exemple, le système informatique douane (SID) approuvé par une loi du 20 décembre 2002, *Mémorial* A 2002, p. 3774.

[8] F. MAIANI, « Le cadre réglementaire des traitements de données personnelles effectuées au sein de l'Union Européenne », *Rev. trim. dr. eur.*, 2002, p. 283, part. p. 286.

La nécessité de trouver un équilibre entre société de l'information et protection de la vie privée a par ailleurs déjà été affirmée dans la convention 108 du Conseil de l'Europe du 28 janvier 1981, entrée en vigueur le 1er octobre 1985, qui énonce au dernier considérant de son préambule « la nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples ».
La directive 95/46/CE, et par conséquent la loi, précisent et amplifient les principes contenus dans la convention 108 du Conseil de l'Europe. Ces trois textes regroupent les règles applicables cumulativement au traitement des données à caractère personnel.

13-3. Si la protection des personnes contre des abus en matière de traitement de données trouve son origine dans le droit au respect à la vie privée inscrit à l'article 8 de la Convention européenne des droits de l'homme, la tendance est de la considérer comme domaine à part entière. Ainsi, l'article 8 de la Charte des droits fondamentaux de l'Union européenne annexée au traité de Nice[9] élève la protection des données à caractère personnel au rang de droit fondamental spécifique. D'un objectif inspiré par des considérations économiques, la protection des données est en train de s'émanciper pour développer un caractère à part, celui d'un droit de l'homme[10].
La technicité de la matière et la recherche d'une bonne compréhension de la loi obligent à déterminer son champ d'application (titre I), afin de permettre l'analyse des conditions du traitement de données à caractère personnel (titre II) et des droits des personnes dont les données font l'objet d'un traitement (titre III). En raison du caractère par essence international de la société de l'information, la loi se devait d'aborder la question du transfert des données vers d'autres États (titre IV). Enfin, les conditions du traitement de données ainsi que le respect des droits des personnes concernées appellent des mécanismes de contrôle et de recours (titre V).

TITRE I
Le champ d'application de la loi

13-4. L'une des critiques récurrentes adressées à la loi est celle d'être une loi « fourre-tout » en raison de son applicabilité horizontale et de sa technicité[11]. Il faut cependant reconnaître que, d'une part, la protection des personnes

[9] *J.O.C.E.* C-364/200, p. 10.
[10] Voy. Premier rapport de la Commission européenne sur la mise en œuvre de la directive relative à la protection des données adopté le 15 mai 2003 COM (2003) 265 final, p. 4.
[11] Avis de la Chambre des fonctionnaires et employés publics, *Doc. parl.* 4735-1, p. 1.

n'aurait pas été facilitée ou rendue plus claire par l'édiction de lois sectorielles dont les champs d'application respectifs auraient pu créer des vides juridiques ou, au contraire, se recouper de manière préjudiciable à la détermination exacte des droits et obligations de chacun. D'autre part, le caractère horizontal du champ d'application de la loi n'empêche pas que des législations à vocation sectorielle puissent s'y greffer. Le considérant 68 de la directive 95/46/CE annonce cette possibilité en disposant que les principes y contenus « pourront être précisés et complétés, notamment pour certains secteurs, par des règles spécifiques ». D'ailleurs, une directive « sectorielle » a été adoptée dans le même domaine des télécommunications et doit être transposée en droit luxembourgeois[12].

L'applicabilité horizontale de la loi a pour conséquence un champ d'application particulièrement vaste[13]. En effet il est aussi bien matériel et personnel (chapitre 1) que territorial (chapitre 2).

CHAPITRE 1
Le champ d'application matériel et personnel

13-5. Le but de la loi est de protéger la « personne concernée » dont les données à caractère personnel font l'objet d'un traitement par le responsable du traitement. Le champ d'application matériel et personnel de la loi dépend donc du contenu des notions de « donnée à caractère personnel » (section 1), de « personne concernée » (section 2), de « responsable du traitement » (section 3) et de « traitement » (section 4).

SECTION 1
La donnée à caractère personnel

13-6. Une donnée à caractère personnel (la « donnée ») est « 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 [la « 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,

[12] Directive 97/66/CE du Parlement européen et du conseil du 15 décembre 1997, *J.O.C.E.* L 24/1998, p. 1 ; projet de loi 5181 déposé le 11 juillet 2003.

[13] On pourrait même se poser la question de savoir si le soucis de prévoir une protection complète n'a pas abouti à un champ d'application qui est trop vaste.

culturelle, sociale ou économique »[14]. L'identification peut se faire par « toute forme de captage, de traitement et de diffusion de sons ou d'images »[15].
Un exemple évident est le numéro de sécurité sociale ou de passeport.
La délimitation de cette notion peut cependant être beaucoup moins aisée. Ainsi, par exemple, si une société établit un organigramme avec, même en chiffres globaux, le nombre de ses salariés et les postes occupés par eux, il n'en demeure pas moins que restent identifiables les personnes occupant seules un poste déterminé. Au contraire, il n'existe *a priori* pas de possibilité d'identification dès lors que l'organigramme fait référence à 354 salariés occupés au sein de l'entreprise. L'identification redevient possible si, suite à une ventilation par activité ou poste, ce même document fait référence, par exemple, à trois salariés occupés au sein du service du contrôle interne, dont le contrôleur interne, une secrétaire et un stagiaire, ces trois personnes étant alors identifiables. Dans ce cas, il importe peu que les postes ne soient indiqués que par un code. En effet, des données codées restent des données tombant sous la définition de l'article 2, lettre (e) « dès lors qu'un moyen raisonnable existe de les ré-identifier »[16].

13-7. Par conséquent, une donnée anonyme ou ayant été rendue anonyme n'est pas considérée comme « donnée » au sens de la loi, dans la mesure seulement où il n'est pas ou plus possible par tout moyen d'identifier la personne à laquelle se rattache cette donnée, c'est-à-dire à la « personne concernée ».

SECTION 2
La personne concernée

13-8. La détermination de la personne concernée est aisée. La personne concernée est la personne dont les données font l'objet d'un traitement. Il peut s'agir d'une personne physique ou morale, de droit public ou de droit privé. Même un groupement de fait dépourvu de personnalité juridique se range dans la définition prévue à l'article 2, lettre (n), de la loi dès lors que ses données font l'objet d'un traitement.

[14] Article 2, lettre (e), de la loi.
[15] Article 2, paragraphe (4), de la loi.
[16] Th. LÉONARD, Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution », *J.T.*, 1999, p. 377, part. note 16.

SECTION 3
Le traitement

13-9. La loi a donné une définition exhaustive de la notion de « traitement ». Il s'agit de « 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 »[17].

13-10. Le traitement est en somme toute opération ayant trait à des données. Il remplace la notion surannée de banque de données utilisée comme référence dans la loi de 1979. Le lieu où sont stockées des données n'a, partant, plus d'importance. C'est ce qui est fait des données et ce à quoi elles servent qui doit être considéré.

13-11. La vaste étendue des opérations couvertes par cette définition englobe également la manière dont ces opérations sont effectuées. Un traitement n'a pas besoin d'être entièrement automatisé pour tomber dans la définition de l'article 2, lettre (s) : « Si au moins une des opérations, dont l'ensemble constitue le traitement [...], est effectué de façon automatisée, les autres l'étant de façon « manuelle », le traitement doit être opéré en conformité avec les dispositions de la présente loi »[18]. Le fait, par exemple, de remplir ou de faire remplir des documents d'ouverture de compte sur des documents préimprimés, et par suite d'enregistrer ces renseignements dans le système informatique de la banque, constitue un traitement. Comme l'usage de l'informatique est devenu chose courante, le nombre d'opérations devant être qualifiées de traitement est immense.
Ceci est d'autant plus vrai que même en présence de traitements non entièrement automatisés, la loi continue à s'appliquer dès lors que des « données [sont] contenues ou [sont] appelées à figurer dans un fichier »[19]. D'après l'article 2, lettre (h), un fichier est « un ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ». Un fichier, fût-il « manuel », peut ainsi être structuré, par exemple par ordre alphabétique ou chronologique.

[17] Article 2, lettre (s), de la loi.
[18] *Doc. parl.* 4735, p. 28.
[19] Article 3, paragraphe (1), de la loi.

Par conséquent, seul un fichier non structuré, en d'autres mots des données en vrac, échappe à la loi. Quelle est cependant l'utilité d'une telle masse non structurée de données ? On pourrait même avancer que c'est en raison de l'inutilité d'une telle masse que la loi n'a pas lieu de s'appliquer.

13-12. Deux catégories de traitements sont expressément exclues du champ d'application *ratione materiae* de la loi. D'une part, il s'agit des traitements mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques. D'autre part, sont exclus les traitements concernant une personne morale dont la publication est requise par la loi ou un règlement. Cette seconde exception, qui n'a été introduite qu'au cours de la discussion du projet de loi en commission, vise en premier lieu les données devant être publiées au *Mémorial* conformément à la loi du 10 août 1915 sur les sociétés commerciales.
La question se pose alors, par exemple, de savoir si les registres d'actionnaires ou d'obligataires d'une société anonyme tombent sous le coup de cette exception. La réponse devrait en principe être négative dans la mesure où il ne s'agit pas d'un traitement devant faire l'objet d'une publication.
En revanche, doivent être exclus du champ d'application de la loi les traitements de données concernant les associés d'une société à responsabilité limitée ainsi que les traitements de données relatives aux commerçants et dirigeants de sociétés commerciales, groupements d'intérêt économique, etc., qui doivent être publiées conformément à la loi du 19 décembre 2002 concernant le registre de commerce et des sociétés.

SECTION 4
Le responsable du traitement

13-13. Le responsable du traitement détermine les finalités du traitement et les moyens pour y parvenir. Il s'agit de celui qui dispose du pouvoir décisionnel en la matière[20]. Ainsi, une SICAV ou une société de gestion d'un FCP est à considérer comme responsable du traitement. La banque dépositaire ou l'agent administratif doit être qualifié de sous-traitant puisqu'il n'est que l'exécutant des ordres du responsable du traitement. L'article 21 de la loi prévoit qu'un sous-traitant ne peut procéder à un traitement que sur ordre du responsable du traitement, sauf en cas d'obligation légale. En outre, l'article 22, paragraphe (3), exige un contrat ou un autre écrit liant le sous-traitant et le responsable du traitement.

[20] *Doc. parl.* 4735-13, p. 6.

Un même traitement peut être effectué conjointement par plusieurs responsables du traitement, par exemple dans le cadre d'une association momentanée ou en participation.
Au vu du champ d'application *ratione personae* et *ratione materiae* très vaste de la loi, il convient de délimiter l'application de la loi de manière territoriale.

CHAPITRE 2
Le champ d'application territorial

13-14. Le champ d'application territorial de la loi revêt une importance particulière au regard de l'objectif initial poursuivi par le législateur communautaire, à savoir l'élimination des obstacles à la circulation des données au sein du marché intérieur. Il serait ainsi préjudiciable pour les intérêts tant de la personne concernée que du responsable du traitement, soit qu'aucune législation relative à la protection des données ne s'applique à un traitement donné, soit, au contraire, qu'un même traitement fasse l'objet d'une application cumulative de plusieurs législations nationales différentes[21].
Ainsi, l'article 3, paragraphe (2), de la loi fixe deux critères successifs pour déterminer si un traitement entre dans son champ d'application. Ces deux critères tournent autour de la localisation du responsable du traitement : la loi s'applique lorsque le responsable du traitement est soumis au droit luxembourgeois (section 1), et au cas où le responsable du traitement est établi hors de la Communauté européenne, dès lors que les moyens de traitement sont situés au Luxembourg (section 2). Ni la localisation de la personne concernée ni le lieu de la collecte ne sont pris en compte.

13-15. Afin d'éviter toute confusion, il convient cependant de souligner que l'article 3, paragraphe (2), ne préjuge aucunement les règles de territorialité prescrites par le droit pénal[22]. Les nombreuses sanctions pénales contenues dans la loi relèvent naturellement des règles générales régissant la compétence des juridictions répressives luxembourgeoises.

[21] *Doc. parl.* 4735-13, p. 7.
[22] Directive 95/46/CE, considérant 21.

SECTION 1
Le responsable du traitement soumis au droit luxembourgeois

13-16. Dès que le responsable du traitement est soumis au droit luxembourgeois, le traitement qu'il met en œuvre relève, lui aussi, du droit luxembourgeois.

Le projet de loi 4735 tel qu'il fut déposé à la Chambre des députés, tout comme l'article 4 de la directive 95/46/CE, font référence au lieu d'établissement du responsable du traitement. C'est à la demande du Conseil d'État, dans un souci de pure simplification rédactionnelle, que la « soumission au droit luxembourgeois » a remplacé le critère de l'établissement initialement utilisé par le gouvernement. Cette substitution n'est qu'apparente et n'a aucune influence sur la portée de l'article 3, paragraphe (2), lettre (a).

Est soumise au droit luxembourgeois toute personne qui est établie, soit au Luxembourg, soit encore en tout lieu où, selon le droit international public, le droit luxembourgeois est applicable. La forme de l'établissement, qu'il s'agisse d'une filiale ou d'une succursale d'une société étrangère, importe peu. Il en va de même du lieu d'établissement du sous-traitant.

Il faut cependant qu'il s'agisse d'un établissement stable. « L'établissement sur le territoire d'un État membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable »[23]. Ainsi, à titre d'exemple, toute entité soumise par la législation luxembourgeoise à l'exigence d'un agrément est à considérer comme personne soumise au droit luxembourgeois au sens de l'article 3, paragraphe (2), de la loi. *A contrario*, les entités établies dans un autre État membre et opérant au Luxembourg par le biais de la libre prestation de services continuent de relever de la législation applicable en matière de protection des données de leur État d'établissement. De même, si des personnes de droit luxembourgeois prestent leurs services en libre prestation de services dans un autre État membre, la loi reste d'application pour l'ensemble de leurs activités, y compris celles exercées dans le cadre de la libre prestation de services.

Si une discussion peut surgir sur la localisation du siège social réel d'une entité[24], l'emploi du critère de l'établissement du responsable du traitement devrait permettre, même en présence de structures sociétaires multinationales, de délimiter clairement la répartition géographique des champs d'application des législations sur la protection des données.

Le rapport de la commission parlementaire[25] donne l'exemple suivant : « Une société établie en France est chargée de la gestion des données relatives au per-

[23] Directive 95/46/CE, considérant 19.

[24] Voy. C.J.C.E., 5 novembre 2002, aff.C-208/00, *Überseering* ; A. SCHNITGER, « *Überseering* : Schluss mit der « Gründungstheorie » im Binnenmarkt », *Internationales Steuerrecht*, 2002, p. 809, J.-M. JONET, « Sociétés commerciales, La théorie du siège réel à l'épreuve de la liberté d'établissement », *J.T.D.E.*, 2003, p. 33.

[25] *Doc. parl.* 4735-13, p. 8.

sonnel de sociétés établies dans d'autres États membres, dont le Luxembourg. Ce sera la loi française sur la protection des données qui s'applique, car l'établissement du responsable du traitement est situé en France. La solution du conflit de lois se résoudra dans cet exemple toujours en faveur de la loi française, même si la société française devait sous-traiter la gestion des données à une société externe implantée au Luxembourg. Le fait que l'ensemble des autres sociétés du groupe bénéficie du travail effectué par la société française n'est pas pris en considération. Si, en revanche, la société luxembourgeoise utilise les données traitées par la société française pour ses propres besoins et donc pour procéder à un traitement particulier, la loi luxembourgeoise retrouvera application, mais uniquement pour ce qui concerne ce nouveau traitement. »

SECTION 2
Les moyens de traitement sont situés sur le territoire luxembourgeois

13-17. L'article 3, paragraphe (2), lettre (b), vise à éviter que le responsable du traitement essaye d'arguer d'un établissement hors de la Communauté européenne pour tenter d'échapper aux règles luxembourgeoises sur la protection des données. En effet, même si tel était le cas, la loi sera toujours d'application, à condition que les moyens de traitement soient situés au Luxembourg. L'acception du « territoire luxembourgeois » utilisé par l'article 3, paragraphe (2), lettre (b), doit inclure naturellement tout endroit où, en application des règles du droit international public, le droit luxembourgeois est applicable. Cette disposition a donc vocation de protéger les personnes concernées contre la délocalisation fictive de l'établissement du responsable du traitement hors de la Communauté européenne.

Encore faut-il définir la notion des « moyens de traitement ». La loi ne donne pas de définition, sauf pour exclure les moyens qui ne sont utilisés qu'à des fins de transit sur le territoire luxembourgeois. La directive 95/46/CE précise que les moyens de traitement peuvent être automatisés ou non. D'après le rapport de la commission des média et des communications de la Chambre des députés[26], le législateur entendait les « moyens de traitement » « de manière large, c'est-à-dire tant des équipements que des moyens en personnel »[27]. Il s'agit de tous les moyens matériels ou en personnel qui permettent au responsable du traitement d'effectuer un traitement ou même une partie de traitement. De toute façon, l'application de ce critère peut s'avérer difficile en raison de son

[26] Rappelons que les travaux préparatoires ne peuvent jamais compléter ou dénaturer un texte, mais peuvent au contraire « servir utilement à mettre en lumière le but de la loi, à éclairer le texte légal et à corroborer les solutions trouvées dans le texte » (P. PESCATORE, *Introduction à la science du droit*, p. 339) ; voy. aussi CE, 15 décembre 1948, *Pas.*, 14, p. 529.

[27] *Doc. parl.* 4735-13, p. 9

caractère imprécis. La Commission européenne n'a pas exclu une clarification de ce critère et si cette clarification ne devait pas être suffisante, « il pourrait s'avérer nécessaire, en temps opportun, de proposer une modification à la directive qui introduirait un type de lien différent pour déterminer la législation applicable »[28].

13-18. Dans l'hypothèse où de tels moyens sont répartis sur le territoires de plusieurs États membres, le danger de la multiplication des lois territorialement applicables, que la loi voulait précisément éviter, ressurgit. Tout en tenant compte des circonstances de l'espèce, la solution, ou du moins un début de solution, pourrait se trouver dans l'adage « l'accessoire suit le principal » : la loi du lieu où se trouvent les éléments matériels et/ou en personnel indispensables ou les plus importants au traitement devrait – toutes proportions gardées – être privilégiée par rapport aux législations des juridictions où ne se rencontrent que des moyens de traitement accessoires ou de moindre importance.

13-19. Le responsable du traitement établi dans un État tiers à la Communauté européenne, mais disposant de moyens de traitement au Luxembourg, doit désigner, par déclaration écrite adressée à la Commission nationale pour la protection des données, un représentant établi au Luxembourg « qui se substitue [à lui] dans l'accomplissement de ses obligations prévues par la présente loi sans [qu'il] soit dégagé de sa propre responsabilité »[29]. Contrairement au chargé de la protection des données[30], aucune autre condition que celle de son établissement au Luxembourg n'est exigée. Il peut s'agir d'une personne physique ou morale, d'un employé du responsable du traitement ou d'un mandataire. Mais quel que soit le régime juridique des relations entre le responsable du traitement et son représentant luxembourgeois, à aucun moment cette substitution ne saurait décharger le responsable du traitement de sa propre responsabilité.
Dès lors que la loi est applicable, le responsable du traitement ne peut procéder à un traitement que si celui-ci satisfait aux conditions posées par la loi, c'est-à-dire s'il est loyal, licite et légitime.

[28] Voy. Premier rapport de la Commission européenne sur la mise en œuvre de la directive relative à la protection des données adopté le 15 mai 2003 COM (2003) 265 final, p. 19.
[29] Article 3, paragraphe (2), alinéa 2, de la loi.
[30] Voy. titre V, chapitre 1, section 2.

TITRE II

Les conditions du traitement

13-20. Dans un souci de protection de la personne concernée, la loi impose à un traitement un certain nombre de conditions de fond qui gravitent toutes autour du principe de finalité (chapitre 1). En outre, même avant de commencer un traitement, le responsable du traitement doit satisfaire à certaines formalités de notification ou d'autorisation (chapitre 2).

CHAPITRE 1

Le principe de finalité

13-21. Des données ne peuvent être traitées qu'en vue d'atteindre un certain but que le responsable du traitement s'est fixé. Le principe fondamental de la finalité du traitement a une portée double : les données doivent être traitées loyalement et licitement (section 1) et le traitement ne peut être effectué que s'il est légitime (section 2). Ces deux conditions sont cumulatives.

SECTION 1

Le traitement loyal et licite

13-22. L'article 4 de la loi oblige le responsable du traitement à s'assurer que les données sont traitées de manière loyale et licite. Il s'agit d'une obligation de moyens[31].
Le paragraphe (1) de l'article 4 énumère, de manière non limitative, les situations dans lesquelles un traitement est mis en œuvre loyalement et licitement.

I. Les données doivent être collectées pour des « finalités déterminées, explicites et légitimes »

13-23. Il s'agit de la consécration expresse du principe de finalité. Le traitement des données ne doit pas être incompatible avec la finalité poursuivie. Avant de commencer un traitement, le responsable du traitement doit savoir à quelle fin il collecte les données. Il ne peut pas commencer un traitement pour ensuite, au vu des données collectées, en déterminer le but. En application de l'article 26 de la loi, le responsable du traitement doit informer, préalablement au traitement, la personne concernée sur la finalité du traitement. Cette

[31] La version initiale du projet de loi 4735 indiquait que le responsable du traitement devait le « garantir », ce qui impliquait une obligation de résultat.

information ne peut se faire utilement que si la finalité est décrite avec suffisamment de précision.
Ni la loi ni la directive 95/46/CE ne contiennent de définition de la notion de finalité. Mais « il ne peut [...] être question d'englober dans une finalité un ensemble d'objectifs flous et trop nombreux »[32]. En fait, il s'agit du but recherché par le responsable du traitement. Il se peut naturellement que le responsable du traitement s'aperçoive en cours de traitement que la finalité recherchée ne sera pas atteinte. Cette circonstance ne devrait en principe pas permettre de considérer rétroactivement que le traitement ne poursuivait aucune finalité.

13-24. Un traitement peut poursuivre plusieurs finalités. De même, une seule et même donnée peut être traitée pour atteindre plusieurs finalités. Par exemple, une société peut envisager la collecte d'un certain nombre de données auprès de ses salariés, d'une part, en vue de remplir ses obligations légales, comme les retenues d'impôts, et, d'autre part, pour l'établissement d'un système d'attribution de primes ou de *stock-options*.
Quel que soit le nombre des finalités poursuivies, il convient d'examiner séparément pour chaque finalité si les conditions d'un traitement licite et loyal et celles d'un traitement légitime sont satisfaites.
Ainsi, pour reprendre l'exemple précédent, si, pour opérer les retenues d'impôts, l'employeur a besoin d'un certain nombre de renseignements sur chaque salarié personne concernée, mais que, pour l'établissement d'un système de primes, des données supplémentaires doivent être traitées, il y aura ainsi deux traitements différents nécessitant deux notifications distinctes. En effet, le traitement de toutes les données sera proportionné par rapport au but de l'élaboration du système de primes, mais il sera disproportionné pour les retenues d'impôts.

13-25. L'article 4, paragraphe (1), précise en outre que les données ne doivent pas être « traitées ultérieurement de manière incompatible avec [les] finalités » initiales. Le rapport de la commission parlementaire s'est fait l'écho d'une controverse en Belgique à propos de la compatibilité automatique en cas de changement de finalité, lorsque ce changement a été rendu nécessaire par la suite en raison d'une nouvelle législation ou réglementation[33]. Une telle compatibilité automatique – telle que prévue par l'article 4 de la loi belge du 11 décembre 1998 – n'a pas été introduite dans la loi, mais « 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 »[34].

[32] A. PIPERS, *Le respect de la vie privée*, cité in *Doc. parl.* 4735, p. 30.
[33] *Doc. parl.* 4735-13, p. 10.
[34] *Ibid.*.

13-26. Un traitement ultérieur peut avoir lieu pour des raisons statistiques, historiques ou scientifiques. Un tel traitement ultérieur, dont le principe est prévu à l'article 4 de la loi, est soumis à un régime particulier, et notamment à une procédure d'autorisation préalable[35].

13-27. Enfin, il va de soi que la finalité ne saurait être contraire à un texte légal ou réglementaire ou à un texte d'origine internationale ou européenne ayant un effet direct au Luxembourg.

II. Les données doivent être « adéquates, pertinentes et non excessives au regard des finalités » poursuivies

13-28. Cette exigence traduit le principe bien connu de la proportionnalité. Le responsable du traitement ne doit traiter que les données nécessaires pour atteindre la finalité qu'il s'est donnée.
Toutes les données collectées ainsi que leur utilisation doivent être en relation avec la finalité poursuivie.

III. Les données doivent être « exactes et, si nécessaire, mises à jour »

13-29. La personne concernée a le droit de faire rectifier les données la concernant qui sont inexactes[36].
Le responsable du traitement doit prendre « toute mesure raisonnable » en vue d'effacer ou de rectifier des données inexactes ou incomplètes au regard de la finalité pour laquelle elles ont été collectées. Malgré cette formulation, le droit d'accès reconnu à l'article 28 de la loi à la personne concernée et la possibilité de contrôle et d'investigation de la Commission nationale pour la protection des données assujettissent le responsable du traitement à une obligation que l'on ne saurait réduire à une simple obligation de moyens. En effet, l'article 28, paragraphe (5), de la loi dispose que « 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* ».

[35] Voy. titre II., chapitre 2, section 2.
[36] Article 28 de la loi.

IV. 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 »

13-30. La durée de conservation des données doit être proportionnée par rapport à la réalisation de la finalité. Il se peut que cette durée, qui doit être communiquée spontanément ou sur demande à la personne concernée et être incluse dans la notification ou dans le demande d'autorisation, ne soit pas connue dès le début.
En effet, comment savoir combien de temps un actionnaire ou un obligataire doit être inscrit au registre des actionnaires ou des obligataires ? Il peut également s'avérer utile ou nécessaire de conserver une quelconque trace de cette détention après que la personne concernée a vendu ses actions ou ses obligations. En outre, des prescriptions légales exigent la conservation de documents pendant un certain délai, ce délai pouvant faire l'objet de suspension, d'interruption, de différents points de départ, etc. Il se peut donc que la durée exacte de conservation des données ne puisse être déterminée avec exactitude. Au regard des circonstances de l'espèce, une attitude réaliste de la Commission nationale pour la protection des données s'impose.
Après avoir examiné comment traiter des données, il s'agit maintenant de déterminer dans quelles hypothèses un traitement peut être effectué.

SECTION 2
Le traitement légitime

13-31. L'examen fouillé des articles 5 et suivants de la loi dépasserait de loin le cadre de la présente contribution. En effet, si l'article 5 fixe les conditions d'ordre général de légitimité d'un traitement, l'article 6 vise les données dites « sensibles », l'article 7 les données médicales, l'article 8 les données judiciaires, l'article 9 la liberté d'expression et les articles 10 et 11 les traitements en vue d'une surveillance. Les articles 10 et 11 faisant l'objet d'un examen séparé, nous nous limiterons aux seules conditions générales et données sensibles des articles 5 et 6.

I. Les conditions générales de légitimité d'un traitement de données

13-32. Contrairement à l'article 4, dont le paragraphe (1) détermine les exigences minimales en matière de qualité des données, l'article 5 énumère de manière limitative les hypothèses dans lesquelles un traitement est légitime.
Un traitement n'est légitime que s'il tombe dans l'une des six hypothèses de l'article 5, paragraphe (1).

A. « Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis »

13-33. Cette cause de légitimité d'un traitement, tirée de l'article 7, lettre (c), de la directive 95/46/CE, s'applique, par exemple, aux données concernant les salariés qu'un employeur doit envoyer aux organismes de sécurité sociale[37] ou aux données inscrites dans un registre des actionnaires exigé par l'article 39 de la loi du 10 août 1915 sur les sociétés commerciales.

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 »

13-34. Cette hypothèse vise le secteur public au sens large du terme.

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 »

13-35. Le traitement est nécessaire pour permettre au responsable du traitement d'exécuter sa partie du contrat. Ainsi, l'ouverture d'un compte bancaire par la personne concernée, cliente du responsable du traitement, oblige celui-ci à traiter les données nécessaires au fonctionnement de ce compte.
Il convient de relever qu'un traitement ne sera légitime, s'agissant de l'exécution de mesures précontractuelles, que si cette exécution a été demandée par la personne concernée.
Le rapport parlementaire souligne qu'en cas de résolution du contrat, le traitement doit immédiatement cesser et les données devront être effacées[38]. Lorsque le contrat est résilié, l'effacement des données ne doit pas revêtir un caractère automatique, mais pourra s'imposer au vu 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 »

13-36. L'équilibre recherché entre les intérêts du responsable du traitement et les droits et libertés fondamentaux de la personne concernée se trouve ici utilement rappelé. Dès que la balance penche en défaveur de la personne concernée, le traitement n'est pas, ou n'est plus, légitime et devra cesser. L'exigence du respect de la balance des intérêts se retrouve implicitement dans les autres hypothèses visées à l'article 5 de la loi.

[37] *Doc. parl.* 4735-13, p. 11.
[38] Sauf naturellement en cas d'un traitement ultérieur pour une finalité historique, statistique ou scientifique.

Dans la mesure où la légitimité du traitement envisagée sous l'optique de l'équilibre des intérêts est largement tributaire des circonstances de l'espèce, une appréciation abstraite doit être relativisée. Ce sera l'examen au cas par cas, sur base des finalités poursuivies par le responsable du traitement, qui sera déterminant. Cependant, un tel examen ne signifie pas que la situation de chaque personne concernée doive être analysée individuellement. C'est l'adéquation entre le traitement en question et la finalité recherchée qui importe.

Ainsi, si les données sont recueillies en vue de l'évaluation d'un crédit ou de la conclusion d'une police d'assurance-vie, il ne faut pas examiner la légitimité dudit traitement par référence à chaque emprunteur ou preneur d'assurance potentiel. Il faut, mais il suffit, que la finalité du traitement puisse être légitime au regard des intérêts du responsable du traitement et des intérêts d'une personne concernée type. Procéder différemment reviendrait à faire analyser pour chaque client ou client potentiel du responsable du traitement, si le traitement est légitime. La surcharge de travail serait alors totalement disproportionnée par rapport au but de la loi.

L'exposé des motifs cite plusieurs exemples, certes abstraits, dans lesquels la balance des intérêts serait respectée[39].

Le premier exemple est celui du traitement dont la finalité est l'évaluation du crédit de la personne concernée « à condition toutefois que [les données] ne soient ni sensibles ni constitutives de profils de la personnalité et qu'elles ne soient communiquées à des tiers que si ceux-ci en ont besoin pour conclure ou exécuter un contrat avec la personne concernée. Toutefois, dès lors que la conclusion du contrat entre la personne concernée et le responsable du traitement, ou encore le tiers auquel les données ont été communiquées, dépend de leur contenu (la personne a-t-elle un crédit suffisant pour bénéficier de tel droit ou contrat, est-elle suffisamment crédible pour bénéficier de telles conditions dans son contrat de prêt, d'assurance automobile, etc. ?), la procédure à suivre sera celle de l'autorisation préalable »[40].

La finalité d'un tel traitement est justement d'évaluer les risques que le responsable du traitement prend s'il conclut un contrat avec la personne concernée. L'article 14, paragraphe (1), lettre (d), de la loi, en prévoyant qu'un traitement peut concerner le crédit et la solvabilité de la personne concernée, pour le soumettre à une autorisation préalable, démontre que cette finalité est légitime en soi. Dans tous les cas, afin de permettre au responsable du traitement d'atteindre la finalité qu'il s'est donnée, la qualité des données devra satisfaire aux conditions de l'article 4 de la loi.

Le second exemple cité concerne le traitement de données à des fins de recherche, de planification ou de statistique. L'exposé des motifs précise que la

[39] *Doc. parl.* 4735, p. 31.
[40] *Eod. loc.*

balance des intérêts serait respectée à condition que « les résultats soient publiés sous une forme ne permettant pas d'identifier les personnes concernées ». Cette condition peut s'avérer impossible à remplir si, par exemple, au sein de l'entreprise, un poste n'est occupé que par un seul salarié. Même en ne citant pas le nom de ce salarié, cette personne est identifiable.
Mais, ici encore, un traitement de données se rapportant aux salariés en vue d'une rationalisation des tâches au sein d'un groupe de sociétés ne devrait pas *a priori* poser des problèmes de légitimité[41]. Le considérant 30 de la directive 95/46/CE permet aux États membres « en vue d'assurer l'équilibre des intérêts en cause, tout en garantissant une concurrence effective [...] [de] 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 ». La planification intragroupe devrait donc être considérée comme un traitement légitime.

E. « Le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée »

Aucune explication ne semble nécessaire à cet égard.

F. « La personne concernée a donné son consentement. »

13-37. Le consentement n'est soumis à aucune forme sacramentelle[42]. Il doit cependant être à la fois exprès, spécifique, non équivoque, libre et informé.
La personne concernée doit savoir à quoi elle s'engage. Elle doit y consentir en connaissance de cause après avoir été informée conformément à l'article 26 de la loi. Elle ne doit pas être contrainte de donner son accord à un traitement. La liberté du consentement s'apprécie au regard des prescriptions des articles 1112 et suivants du Code civil[43].
Si l'on veut légitimer un traitement par le consentement de la personne concernée, il est plus judicieux de stipuler dans un contrat que la personne concernée donne son accord au traitement envisagé, plutôt que de mentionner que le traitement est légitime jusqu'à ce que la personne concernée retire son consentement.
Aux conditions générales de légitimité s'ajoutent des conditions plus spécifiques pour les données dites sensibles.

II. Les conditions de légitimité de traitement des données sensibles

13-38. Les traitements des données sensibles tombent dans le champ d'application de l'article 6 de la loi.
Outre l'interdiction des traitements des données relatives à la santé et à la vie sexuelle de la personne concernée et de ceux concernant les données

[41] *Doc. parl.* 4735-13, p. 13.
[42] *Doc. parl.* 4735-13, p. 4.
[43] *Doc. parl.* 4735-13, p. 5.

génétiques[44], l'interdiction édictée à l'article 6, paragraphe (1), de la loi s'étend aux traitements des données lorsque ces traitements révèlent « l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale » de la personne concernée.
La formulation utilisée tient compte d'une critique adressée à l'endroit de la loi belge du 11 décembre 1998. La loi belge dispose que les données sensibles sont les données qui révèlent l'origine raciale ou ethnique, les convictions religieuses ou philosophiques, etc., de la personne concernée. La loi exige que ce soit le traitement, et non pas la donnée en soi, qui révèle un caractère sensible. Il n'y a donc pas de donnée sensible en soi, même si le langage courant y fait référence.
Ainsi peut-on légitimer le traitement par un employeur d'un chèque adressé à une organisation syndicale et portant la mention « cotisation » : la finalité du traitement ne doit pas être de déterminer, ne serait-ce que de manière indirecte, qui des employés est syndiqué et qui ne l'est pas. « Conformément au principe de finalité, c'est la finalité qui fera qu'un 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. C'est n'est donc pas parce que l'on est en présence de données sensibles que tout traitement est *ipso facto* interdit »[45].
Si un seul et même traitement tombe pour partie sous l'une des conditions de légitimité de l'article 5 de la loi, comme l'exécution d'un contrat, mais si ce traitement inclut aussi des données de santé, le traitement de ces dernières doit être légitimé séparément, par exemple par le biais du consentement de la personne concernée. Si ce traitement est légitimé par le consentement de la personne concernée au regard tant de l'article 5 que de l'article 6 de la loi, un second consentement est superflu, mais il est recommandé de préciser que le consentement englobe les données dites « sensibles ».

13-39. L'article 6 de la loi prévoit cependant un certain nombre d'exceptions dans lesquelles des données dites « sensibles » peuvent être traitées. Il s'agit, par exemple, des procédures judiciaires, de la sauvegarde des intérêts vitaux de la personne concernée, d'un motif d'intérêt public ou des données manifestement rendues publiques par la personne concernée[46].

[44] Le traitement de données génétiques n'a pas été envisagé par la directive 95/46/CE. L'article 6, paragraphe (4), de la loi détermine les cas où un traitement de données génétiques est autorisé : consentement de la personne concernée, procédures judiciaires civiles ou répressives, autorisation par règlement grand-ducal, protection des intérêts vitaux de la personne concernée ou d'un motif d'intérêt public, ou traitement des données génétiques par les services de la santé.
[45] *Doc. parl.* 4735-13, p. 13.
[46] Par exemple, un homme politique a nécessairement, à un moment ou à un autre, comme lors d'élections, mentionné son appartenance à un parti politique, à un syndicat, ou a publiquement fait connaître ses convictions religieuses ou philosophiques.

13-40. Il convient de brièvement décrire deux exceptions qui risquent d'être invoquées pour légitimer le traitement de données « sensibles » : le consentement de la personne concernée[47] et les obligations et droits spécifiques du responsable du traitement, notamment en matière de droit du travail dans la mesure où le traitement est autorisé par la loi[48].

13-41. Le consentement de la personne concernée doit répondre aux mêmes critères que ceux exigée pour son consentement en vue de la légitimité d'un traitement de données en application de l'article 5. L'article 6 ajoute que le consentement de la personne concernée ne permet pas de légitimer un traitement contraire à une loi ou qui, comme en matière de clonage, violerait le principe de l'indisponibilité du corps humain.

13-42. La deuxième exception, relative aux obligations et droits spécifiques en matière du droit du travail, n'est, à l'heure actuelle, d'aucune utilité en droit luxembourgeois. Elle a cependant été incluse dans la loi parce qu'elle était prévue à l'article 8, paragraphe 2., lettre b, de la directive 95/46/CE.
Une fois que le responsable du traitement a déterminé la ou les finalités du traitement, les causes de légitimité de celui-ci ainsi que les données qu'il entend voir traiter, il faut qu'il entreprenne des démarches administratives auprès de l'autorité de surveillance, la Commission nationale pour la protection des données (la « Commission nationale »).

CHAPITRE 2
Les formalités de mise en œuvre du traitement

13-43. Les articles 12 à 15 de la loi organisent les formalités administratives à accomplir avant la mise en œuvre d'un traitement. Contrairement à la loi du 31 mars 1979, qui prévoyait exclusivement une procédure d'autorisation pour toutes les banques de données, la loi ne soumet les traitements à une autorisation préalable que dans certains cas exceptionnels (section 2), le principe étant une simple notification (section 1). Partant, tout traitement qui n'a pas besoin d'une autorisation doit « seulement » être notifié à la Commission nationale.

13-44. Les notifications et autorisations sont renseignées sur un registre public qui peut être consulté en ligne et dont chacun peut prendre connaissance, à l'exception naturellement des indications sur la sécurité des traitements[49]. De

[47] Article 6, paragraphe (2), lettre (a).
[48] Article 6, paragraphe (2), lettre (b).
[49] Article 15, paragraphe (4).

même, l'article 15, paragraphe (5), permet à la Commission nationale de limiter la consultation de ce registre pour les mêmes raisons que celles qui motivent les restrictions au droit d'accès de la personne concernée[50].

SECTION 1
La notification préalable du traitement

13-45. Avant sa mise en œuvre, le traitement est notifié par le responsable du traitement à la Commission nationale. Ceci permettra à cette dernière d'exercer un contrôle *ex post*.
Les formulaires de notification peuvent être téléchargés du site Internet de la Commission nationale[51]. Conformément à l'article 43, paragraphe (2), de la loi, les traitements doivent être notifiés à la Commission nationale dans les quatre mois de la publication d'une notice annonçant la mise à disposition des formulaires. Les notifications pour traitements existants ont dû être accomplies avant le 11 août 2003.
Des traitements relevant d'un même responsable du traitement et poursuivant des finalités identiques ou liées entre elles, peuvent faire l'objet d'une notification unique. L'article 12, paragraphe (2), de la loi permet à la Commission nationale de publier des directives en vue d'une notification simplifiée pour les traitements « dont la mise en œuvre n'est pas susceptible de porter atteinte aux libertés et droit fondamentaux, et notamment à la vie privée, des personnes concernées ». Par délibérations du 1er août 2003, la Commission nationale a adopté six directives permettant des notifications simplifiées des traitements concernant :

– la gestion des membres des fondations et associations sans but lucratif et des associations de fait ;
– l'administration du personnel ;
– les registres des actionnaires ;
– la gestion des contacts et des relations publiques, sociales et professionnelles ;
– l'administration des fournisseurs, y compris la prospection de fournisseurs potentiels ;
– l'administration de la clientèle, y compris la prospection de nouveaux clients, le marketing et la publicité personnalisée.

13-46. Si l'obligation de notification est la règle, certains traitements (outre les traitements qui doivent faire l'objet d'une procédure d'autorisation) échappent à la procédure de notification.

[50] Voy. titre III, chapitre 2.
[51] www.cnpd.lu.

Il s'agit des traitements de données judiciaires prévus à l'article 8 de la loi ainsi que des traitements soumis à la surveillance d'un chargé de la protection des données[52].

Sont également exemptés de toute procédure les traitements « ayant pour seul objet que 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 ».

Est d'abord et avant tout visé par cette disposition inscrite à l'article 12, paragraphe (3), de la loi, le registre du commerce et des sociétés.

Les registres des actionnaires ou des obligataires peuvent-ils de même être considérés comme des registres exemptés de notification ? S'il ne s'agit pas de registres destinés à l'information du public et ouvert à la consultation du public, ils sont tout de même accessibles à toute personne justifiant d'un intérêt légitime, qui est présent en l'occurrence du moment que le demandeur justifie de sa qualité d'actionnaire ou d'obligataire, selon le cas.

Que faut-il entendre par registre destiné à l'information du public, mais qui ne serait accessible que par une personne justifiant d'un intérêt légitime ? Ne pourrait-on, sinon ne devrait-on pas, interpréter l'article 12, paragraphe (3), comme visant non seulement les registres ouverts au public et destinés à l'information du public, mais aussi ceux qui ne sont accessibles qu'aux personnes justifiant d'un intérêt légitime, car destinés à leur information et non pas à celle du public ?

On peut difficilement imaginer qu'un registre ne soit accessible qu'à certaines catégories de personnes tout en poursuivant un but d'information générale. De deux choses l'une : soit le registre est ouvert à tout le monde, et son but d'informer le public peut être réalisé ; soit il n'est ouvert qu'à certains et, partant, son but n'est que l'information de ceux qui y ont accès. Dans la première catégorie se range le registre du commerce et des sociétés, dans la seconde, les registres des actionnaires ou des obligataires.

La Commission nationale estime cependant que les registres des actionnaires ou des obligataires ne bénéficient pas de l'exemption de l'article 12, paragraphe (3), de la loi, mais elle a prévu une notification simplifiée, au moins pour les registres des actionnaires. Compte tenu de la nature des informations qui figurent dans un tel registre et qui sont peu attentatoires à la vie privée des personnes qui y sont répertoriées, il se pose la question de savoir si une modification de la loi ne s'impose pas[53] [54].

[52] voy. titre V, chapitre 1. section 2.

[53] Dans la mesure où certains autres défauts de jeunesse justifient une revue de la loi, ceci pourrait faire partie des modifications à entreprendre.

[54] Il convient cependant de noter que l'article 12, paragraphe (3), de la loi a repris textuellement l'article 18, paragraphe 3. de la directive 95/46/CE.

13-47. Les traitements, qui ne tombent pas sous l'obligation de notification ou qui ne sont pas exempts de notification, doivent être préalablement autorisés.

SECTION 2
L'autorisation préalable du traitement

13-48. La loi prévoit deux catégories différentes d'autorisations préalables.

13-49. La première est prévue à l'article 17 de la loi et concerne les traitements devant être autorisés par voie de règlement grand-ducal. Il s'agit surtout des traitements effectués liés à la prévention, à la recherche et la constatation d'infractions pénales.

13-50. La seconde catégorie de traitements soumis à autorisation est celle pour lesquels une autorisation préalable de la Commission nationale est requise. Il s'agit de traitements « susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées »[55]. Les douze traitements visés sont énumérés à l'article 14, paragraphe (1), de la loi. Il s'agit avant tout du traitement de données « sensibles », y compris les traitements de données « sensibles » pour lesquels la personne concernée a donné son consentement[56] ou les données « sensibles » manifestement rendues publiques par la personne concernée[57]. De même, les traitements effectués aux fins de surveillance de l'article 10 et aux fins de surveillance du lieu de travail de l'article 11 doivent être autorisés.
Sont également soumis à cette procédure les traitements concernant le crédit et la solvabilité des personnes concernées. Au cours des travaux parlementaires, il a été envisagé de ne soumettre à une procédure d'autorisation ces traitements que lorsqu'ils sont mis en œuvre par des personnes autres que les établissements de crédit, au motif que ces derniers étaient soumis à un contrôle de la CSSF. Cette exclusion a été abandonnée, dans la mesure où le contrôle de la CSSF ou du Commissariat aux assurances si l'on y avait ajouté les compagnies d'assurances, n'a pas pour objet d'autoriser les traitements mis en œuvre et de contrôler le respect des dispositions de la loi.
Les traitements concernant l'interconnexion de données doivent aussi être autorisés par la Commission nationale. L'interconnexion de données prévue à l'article 16 de la loi et qui n'est pas régie spécifiquement par un texte légal ou réglementaire, tombe sous le champ d'application de l'article 14 de la loi. Une interconnexion est « toute forme de traitement qui consiste en la corrélation de

[55] Article 20 de la directive 95/46/CE.
[56] Article 6, paragraphe (1), lettre (a), de la loi.
[57] Article 6, paragraphe (2), lettre (e), de la loi.

données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d'autres responsables du traitement »[58]. L'interconnexion peut concerner des traitements autorisés par et/ou notifiés à la Commission nationale. Il doit être possible d'introduire une demande d'interconnexion concomitamment avec une ou plusieurs demandes d'autorisation ou une ou plusieurs notifications.
La finalité poursuivie par l'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 »[59].
Les finalités des traitements dont l'interconnexion est demandée doivent être identiques ou liées.
Finalement, la Commission nationale doit également autoriser les traitements de données collectées pour une finalité déterminée, mais destinées à être traités ultérieurement pour des fins historiques, statistiques ou scientifiques, ainsi que les données utilisées à des fins autres que celles pour lesquelles elles ont été collectées. Dans ce dernier cas, l'article 14, paragraphe (1), lettre (e), ajoute qu'un tel traitement doit recueillir le consentement préalable de la personne concernée. Si celle-ci est décédée, le consentement devra être donné par ses héritiers.

13-51. En ce qui concerne la procédure d'autorisation, la Commission nationale peut 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. Puisque l'autorisation est préalable au commencement du traitement, le responsable du traitement doit s'engager formellement à effectuer le traitement en conformité avec l'autorisation qui lui a été délivrée.
Le contenu d'une demande en autorisation est similaire à celui d'une notification. Cependant, les informations relatives aux données concernées, aux traitements envisagés et aux mesures de sécurité doivent être plus détaillées que dans le cadre d'une notification. L'article 14, paragraphe (2) lettres (e) et (i), en requérant des descriptions détaillées, se montre plus exigeant que l'article 13 traitant du contenu des notifications.
Ayant déterminé le champ d'application de la loi ainsi que les procédures administratives préalables au traitement, il convient de se tourner vers les droits des personnes concernées.

[58] Article 2, lettre (j), de la loi.
[59] *Doc. parl.* 4735-13, p. 30.

TITRE III

Les droits des personnes concernées

13-52. La recherche d'un équilibre entre les intérêts du responsable du traitement et les droits et libertés fondamentaux de la personne concernée exige que cette dernière jouisse d'un certain nombre de droits au regard de ses données qui font l'objet d'un traitement. Il s'agit du droit à l'information (chapitre 1), du droit d'accès (chapitre 2) et du droit d'opposition (chapitre 3).

CHAPITRE 1

Le droit à l'information

13-53. La personne concernée doit savoir que ses données font l'objet d'un traitement (section 1). Le traitement loyal des données l'exige[60]. Cependant, le principe de l'information n'est pas absolu et connaît un certain nombre d'exceptions (section 2).

SECTION 1

Le principe du droit à l'information

13-54. Le droit à l'information est prévu à l'article 26 de la loi. Le législateur luxembourgeois a transposé littéralement les articles 10 et 11 de la directive 95/46/CE.

Lorsque des données sont collectées directement auprès de la personne concernée, le responsable du traitement doit, au plus tard lors de la collecte des données, fournir à cette personne concernée les informations énumérées à l'article 26, paragraphe (1), de la loi :

« (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. »

[60] Considérant 38 de la directive 95/46/CE.

13-55. La liste des informations supplémentaires n'est pas exhaustive. Le responsable du traitement devra fournir toutes les informations supplémentaires nécessaires au regard des circonstances de la collecte des données ou de la finalité du traitement. Ainsi, l'article 30, paragraphe (1), lettres (b) et (c), de la loi oblige par exemple 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. Le fait que la personne concernée puisse consulter le registre public ne dispense pas le responsable du traitement de lui fournir une information complète.

13-56. Si les données ont été collectées non pas auprès de la personne concernée, mais auprès d'une personne tierce, peu importe que cette personne soit liée à la personne concernée ou non, le responsable du traitement doit fournir directement à la personne concernée les informations précitées[61] « 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 »[62], afin de lui permettre de faire usage de ses droits d'accès ou d'opposition.

13-57. L'obligation d'informer la personne concernée est dite constituer une obligation de résultat[63] [64].
Aucune exigence légale ne concerne la manière dont les informations ont été fournies à la personne concernée. Mais il faut, d'abord, que l'information soit intelligible. Une information orale peut suffire. Ensuite, l'information doit être fournie directement à la personne concernée et doit donc être ciblée. Si une information publiée dans un ou plusieurs quotidiens ne saurait suffire pour satisfaire aux exigences de l'article 26, il convient cependant de relever qu'une information publiée dans un prospectus ou autre document soumis à la personne concernée, même si celle-ci n'y appose pas sa signature, doit être considérée comme suffisante au regard des prescriptions de l'article 26. Enfin, lorsqu'il est question de « finalités déterminées », l'intention du législateur était justement d'éviter des informations portant sur des finalités vagues[65].

13-58. En cas de contestation sur l'existence ou l'étendue de l'information fournie à la personne concernée, la charge de la preuve du respect des dispositions de l'article 26 pèse sur le responsable du traitement.
L'obligation positive d'information connaît cependant un certain nombre d'exceptions.

[61] À l'exclusion naturellement de l'information sur le caractère obligatoire ou facultatif des réponses et des conséquences d'un éventuel défaut de réponse.
[62] Article 26, paragraphe (2), de la loi.
[63] *Doc. parl.* 4735-13, p. 24.
[64] Le doute quant à la justification d'une telle qualification reste cependant permis.
[65] *Doc. parl.* 4735-13, p. 24.

SECTION 2
Les exceptions au droit à l'information

13-59. Les exceptions au droit d'information se retrouvent aux articles 26 et 27 de la loi

I. Les exceptions de l'article 26 de la loi

13-60. Deux exceptions résultent du libellé de l'article 26 de la loi.
Le responsable du traitement est dispensé d'informer la personne concernée au cas où celle-ci a déjà été informée avant la collecte ou, le cas échéant, dès l'enregistrement des données ou au plus tard lors de la première communication de données. Selon les circonstances, un complément d'information peut cependant s'avérer nécessaire. « Par ailleurs, l'exception ne joue que si la personne concernée est informée, non si elle est raisonnablement supposée être informée »[66].
Ensuite, l'article 26 de la loi dispose que le droit à l'information ne joue qu'en cas de *collecte* des données. Si les données ont été volontairement et spontanément fournies par la personne concernée, le droit à l'information n'aurait pas de sens. Si cette communication volontaire et spontanée émane, en revanche, d'une tierce personne, la personne concernée devra toujours être informée selon les modalités de l'article 26, paragraphe (2).

II. Les exceptions de l'article 27 de la loi

13-61. Ces exceptions sont au nombre de trois.
D'abord, l'article 27, paragraphe (1), de la loi écarte le droit à l'information, lorsque le traitement est nécessaire pour sauvegarder :

« (a) la sûreté de l'État ;
(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[67], 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'État 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. »

[66] Th. Léonard, Y. Poullet, *op. cit.*, p. 389.
[67] Voy., par exemple, article 39 de la loi du 5 avril 1993 sur le secteur financier.

Ensuite, l'article 27, paragraphe (2), concerne la liberté d'expression dont l'article 9 organise un régime à part.
Enfin l'article 27, paragraphe (3), fait exception au droit à l'information « 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 »[68].
Non seulement la personne concernée a le droit de recevoir un certain nombre d'informations avant que le traitement ne commence, mais elle peut, pendant le traitement de ses données, avoir accès à celles-ci.

CHAPITRE 2
Le droit d'accès

13-62. Même après la collecte des données, la personne concernée garde une certaine emprise sur ses données par le biais de son droit d'accès. Ce droit lui permettra de vérifier si les données sont effectivement traitées conformément aux informations qui lui ont été fournies et conformément à la loi. À l'instar du droit à l'information, le principe du droit d'accès (section 1) souffre un certain nombre d'exceptions (section 2).

SECTION 1
Le principe du droit d'accès

13-63. L'article 28 de la loi autorise la personne concernée ou ses ayants droit à condition que ceux-ci justifient d'un intérêt légitime, à 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 ;

[68] Considérant 40 de la directive 95/46/CE.

(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 ».

13-64. Le droit d'accès est cependant subordonné à la condition que la personne concernée ou ses ayants droit prouvent leur identité. En application de l'article 28, paragraphe (8), toute personne qui prend sciemment un nom ou un prénom supposé ou une fausse qualité pour obtenir communication de données est punie d'un emprisonnement de huit jours à un an et/ou d'une amende de 251 à 125 000 euros.

13-65. 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[69].

13-66. Le responsable du traitement est tenu de rectifier, effacer ou verrouiller les données qui n'ont pas été traitées en conformité avec la loi. Faute de ce faire, la Commission nationale peut sanctionner le responsable du traitement et ordonner l'interdiction temporaire ou définitive du traitement ou même la destruction des données.
Le paragraphe (7) de l'article 28 exige que la rectification, l'effacement ou le verrouillage soit notifié sans délai par le responsable du traitement aux destinataires auxquels les données ont été communiquées. Le responsable du traitement n'est pas obligé de procéder à cette notification si cette dernière s'avère impossible, c'est-à-dire si une telle notification ne peut avoir lieu pour des raisons matérielles ou techniques. Un coût trop élevé ou exigeant des efforts disproportionnés ne peut cependant pas exonérer le responsable du traitement de la notification[70].
Si le droit d'accès est le principe, il est assorti de certaines exceptions. La loi a repris et précisé les exceptions au droit d'accès prévues dans la directive 95/46/CE.

[69] Article 28, paragraphe (6), de la loi.
[70] *Doc. parl.* 4735-13, p. 26.

SECTION 2

Les exceptions au droit d'accès

13-67. Les exceptions au droit d'accès sont similaires à celles visant le droit à l'information, à savoir notamment la liberté d'expression, la sûreté de l'État, la défense, la sécurité publique, la prévention, la recherche, la constatation et la poursuite d'infractions pénales, y compris la lutte contre le blanchiment, ou le déroulement de procédures judiciaires, un intérêt économique ou financier important de l'État ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal, ou la protection de la personne concernée ou des droits et libertés d'autrui.
L'article 29, paragraphe (2), permet encore de limiter le droit d'accès en présence de données traitées exclusivement à des fins de recherche scientifique ou de données stockées pour une durée n'excédant pas celle nécessaire à la seule finalité d'établissement de statistiques, ou quand il n'existe manifestement aucun risque d'atteinte à la vie privée d'une personne concernée, ou encore quand les données ne peuvent être utilisées aux fins de prendre une mesure ou une décision se rapportant à des personnes précises.

13-68. Le responsable du traitement doit toujours indiquer au demandeur les raisons de la limitation du droit d'accès. S'il ne fait que différer l'exercice de ce droit, le responsable du traitement doit indiquer la date à partir de laquelle le droit d'accès peut à nouveau être exercé[71].
La Commission nationale, qui est informée du refus de donner accès, peut alors exercer son pouvoir d'investigation et peut faire opérer la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la loi. En outre, la Commission nationale peut, mais n'est pas obligée d'informer la personne concernée du résultat de ses investigations, « sans toutefois mettre en danger la ou les finalités des traitements en question. ».
Outre son droit d'information et son droit d'accès, la personne concernée peut s'opposer à certaines utilisations de ses données.

CHAPITRE 3

Le droit d'opposition

13-69. Le droit d'opposition, qui n'existait pas sous l'empire de la loi du 31 mars 1979, concerne soit une donnée déterminée, soit un traitement mis en œuvre à des fins de prospection.

[71] Article 29, paragraphe (3), de la loi.

L'article 30 de la loi permet à la personne concernée de s'opposer à ce que des données la concernant fassent l'objet d'un traitement, à moins qu'un tel traitement ne soit prévu par une disposition légale. L'opposition doit être motivée « pour des raisons prépondérantes et légitimes tenant à [la] situation particulière » de la personne concernée. Si l'opposition est déclarée fondée, soit par le responsable du traitement auquel l'opposition est envoyée, soit par la Commission nationale si celle-ci a dû intervenir, le traitement peut certes continuer, mais il ne peut porter sur les données litigieuses.
L'article 30 vise également les traitements réalisés à des fins de prospection. La personne concernée, dûment informée de la finalité prospective du traitement et de l'existence de son droit d'opposition, peut s'opposer gratuitement au traitement en tant que tel. La loi vise toute forme de prospection, même celle à but non commercial[72].
La loi vise à concilier la libre circulation des données et la protection des personnes concernées. Un des domaines où cet objectif a été le plus difficile à atteindre – et l'a-t-il d'ailleurs été ? – est les transferts internationaux de données vers des pays tiers.

TITRE IV

Les transferts de données vers des pays tiers

13-70. Les transferts de données entre États membres ne devraient pas poser de problèmes particuliers, vu que tous les États membres de l'Union européenne sont censés avoir transposé la directive 95/46/CE[73].
En revanche, les transferts de données vers des pays tiers, c'est-à-dire des pays qui ne sont pas membres de l'Union européenne[74], mérite un développement à part et beaucoup plus fouillé, vu la complexité et l'importance de cette question. En effet, « le partage et la communication internationale de données sont devenus la règle et non l'exception »[75]. Faire abstraction de cette réalité aurait condamné la directive 95/46/CE, et par ricochet la loi, à rester définitivement lettre morte avant même son application. D'un autre côté, de tels transferts comportent, du moins en puissance, les dangers les plus importants pour la

[72] *Doc. parl.* 4735-13, p. 27.
[73] Même s'il découle du premier rapport de la Commission européenne sur la mise en œuvre de la directive 95/46/CE adopté le 15 mai 2003 que des différences, parfois assez substantielles, existent au niveau de la transposition de cette directive dans les législations des États membres.
[74] Certains États membres ont élargi la définition de pays tiers, en les définissant comme étant tous les pays qui ne sont pas membres de l'EEE.
[75] HAVELANGE, LACOSTE, « Les flux transfrontaliers de données à caractère personnel en droit européen », *J.T.D.E.*, 2001, p. 241.

protection des données, car, suite à une diffusion de plus en plus large de ses données, la personne concernée risque d'en perdre définitivement la maîtrise.
La question du transfert de données vers des pays tiers est réglée par les articles 18 et 19 de la loi qui sont la reproduction quasi littérale des articles 25 et 25 de la directive 95/46/CE. L'article 18 de la loi prévoit le principe que des données ne peuvent être transférées vers un pays tiers que si ce dernier assure une protection adéquate (chapitre 1). Les exceptions à ce principe se retrouvent à l'article 19 (chapitre 2).

CHAPITRE 1
Le principe : le transfert vers les seuls pays assurant un niveau de protection adéquat

13-71. Le principe posé par l'article 18 de la loi semble être judicieux : 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 »[76].
Par voie de conséquence, comme le rappelle l'article 18, paragraphe (4), de la loi, un transfert de données vers un pays n'assurant pas un tel niveau de protection adéquat est interdit.

13-72. Le pays tiers qui est visé est le pays de la destination finale[77]. C'est lui dont la législation doit assurer ce niveau de protection adéquat.
La notion de protection adéquate n'a pas reçu de définition ni dans la directive 95/46/CE ni dans la loi. L'article 18, paragraphe (2), de la loi donne cependant des lignes directrices au responsable du traitement. Celui-ci 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 ».
Par conséquent, la protection adéquate oblige non pas le responsable du traitement à examiner si la législation ou les règles professionnelles applicables dans le pays de destination correspondent mot pour mot aux prescriptions contenues dans la loi, mais plutôt à vérifier si cette législation ou ces règles permettent d'assurer de manière adéquate la protection des personnes concernées en cas de traitement de données à caractère personnel. Sous cet aspect, tenant compte de l'objectif poursuivi, à savoir la protection des personnes concernées,

[76] Article 18, paragraphe (1), de la loi.
[77] *Doc. parl.* 4735-13, p. 42.

les termes de « protection adéquate » peuvent s'interpréter comme une protection « équivalente », utilisés dans la convention 108 du Conseil de l'Europe. La pratique de la Commission européenne, qui en vertu de l'article 25, paragraphe 6, de la directive 95/46/CE, a constaté que certains pays tiers assurent un niveau de protection adéquat[78], confirme cette approche, qui est d'ailleurs la seule approche réaliste possible en la matière.
Le groupe prévu à l'article 29 de la directive 95/46/CE a établi une méthodologie et des critères d'appréciation du caractère adéquat de la protection[79]. « Le responsable du traitement peut légitimement s'inspirer de ces critères »[80].

13-73. Il appartient d'abord au responsable du traitement d'apprécier le caractère adéquat de la protection assurée dans le pays tiers où il entend transférer les données qu'il a traitées.
« En cas de doute », l'article 18, paragraphe (3), de la loi lui offre la possibilité de saisir la Commission nationale à qui il incombera d'apprécier si un transfert de données vers un pays tiers est permis en application de l'article 18 de la loi[81].
La Commission nationale informera la Commission européenne des pays au sujet desquels elle a constaté l'absence d'un niveau de protection adéquat.
La Commission européenne peut elle aussi constater qu'un pays tiers assure un niveau de protection adéquat. Les États membres sont obligés de se conformer à la décision de la Commission européenne[82]. Conformément à l'article 25, paragraphe 4, de la directive 95/46/CE, si la Commission européenne estime qu'un pays tiers n'assure pas la protection adéquate requise, les États membres devront interdire tout transfert de données vers ce pays, à moins qu'un transfert de données vers un tel pays puisse être légitimé par l'une des exceptions prévues à l'article 19 de la loi.
La Commission européenne aura donc toujours le dernier mot pour agréer un pays tiers et lui certifier une protection adéquate des personnes concernées.
Au jour de la rédaction de la présente contribution, la Commission européenne a admis dans le cercle restreint des pays tiers autorisés, les législations suisse[83], hongroise[84], canadienne[85] et argentine[86].
En outre, le 26 juillet 2000[87], la Commission européenne a décidé que les principes de la « sphère de sécurité » (*safe harbour*) édictés par le ministère

[78] Voy. nº 73, ci-après.
[79] Document de travail adopté le 24 juillet 1998 ; publié sous :
www.europa.eu.int/comm/ internal_market/en/dataprot/wpdocs/index.htm
[80] *Doc. parl.* 4735-13, p. 42.
[81] Voy. article 18, paragraphe (4), de la loi.
[82] Article 25, paragraphe 6, de la directive 95/46/CE.
[83] Décision de la Commission 2000/518/CE du 26 juillet 2000, *J.O.C.E.* L 215/1.
[84] Décision de la Commission 2000/519/CE du 26 juillet 2000, *J.O.C.E.* L 215/4.
[85] Décision de la Commission 2002/2/CE du 20 décembre 2001, *J.O.C.E.* L 2/13.
[86] Décision de la Commission C (2003) 1731 du 30 juin 2003.
[87] Décision de la Commission 2000/520/CE, *J.O.C.E.* L 215/7.

américain du Commerce remplissent les critères de protection adéquate[88]. Si une société américaine adhère aux principes de la « sphère de sécurité », elle peut importer des données en provenance, même indirecte, d'un État membre de l'Union européenne. Mais seules les sociétés qui relèvent de la compétence de la Federal Trade Commission ou du ministère américain des Transports peuvent participer à la « sphère de sécurité ». Par conséquent, le secteur bancaire tout comme celui des télécommunications y échappent, ce qui constitue sans nul doute une grave lacune.
Le groupe de travail prévu à l'article 29 de la directive 95/46/CE, qui a pour mission de donner à la Commission européenne un avis sur le niveau de protection dans la Communauté européenne et dans les pays tiers, a positivement avisé la législation de Guernesey[89].

13-74. Les mécanismes d'agrément de la protection adéquate offerte par un pays tiers risquent de ne pas se révéler satisfaisants.
D'abord, le responsable du traitement ne dispose pas de toutes les informations nécessaires pour apprécier le caractère adéquat d'une protection de données existant dans un pays tiers. Il pourra également se montrer réticent à prendre une décision, de peur de voir engager sa responsabilité en cas de mauvaise appréciation de sa part.
De son côté, la Commission nationale risque de se trouver fort embarrassée par certaines demandes de confirmation émanant de responsables du traitement. En effet, elle doit certes se conformer aux décisions de la Commission européenne sur le niveau de protection adéquat et respecter les dispositions de la loi. Mais si elle adopte une attitude trop stricte, les dommages pour le commerce international et les réseaux de télécommunications seront à ce point importants que la loi risquera de ne plus être appliquée, à l'instar de la loi de 1979. À l'autre extrême, une attitude trop laxiste aura pour conséquence un affaiblissement de la protection des données.
Quant à la Commission européenne, à court et moyen terme elle ne prévoit des agréments que pour un nombre limité de pays[90]. Ceci ne rendra pas plus facile le travail du responsable du traitement ou de la Commission nationale. C'est dans pareille situation que les exceptions prévues à l'article 19 de la loi pourront se montrer plus efficaces.

[88] Pour une description de cette décision : HAVELANGE, LACOSTE, *op. cit.*, p. 244 et s.
[89] Avis 5/2003 du 13 juin 2003.
[90] Considérant 4 de la décision de la Commission européenne 2001/497/CE du 15 juin 2001, *J.O.C.E.* L 181/19.

CHAPITRE 2
Les exceptions : les transferts vers des pays n'assurant pas un niveau de protection adéquat

13-75. L'article 19 de la loi prévoit deux catégories d'exceptions au principe de l'interdiction du transfert vers un pays tiers n'assurant pas un niveau de protection adéquat.
D'abord, un tel transfert est permis dans certaines situations limitativement énumérées à l'article 19, paragraphe (1), c'est-à-dire lorsque :

a. la personne concernée a donné son consentement au transfert envisagé ;
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), de la loi.

L'article 19, paragraphe (2), précise que s'il fait usage d'une de ces conditions de légitimation, le responsable du traitement doit notifier à la Commission nationale un rapport établissant les conditions dans lesquelles le transfert vers le pays tiers en question a été effectué. Cette obligation ne se retrouve pas telle quelle dans la directive 95/46/CE. Certes, l'article 19, paragraphe (2), de la loi peut laisser entendre qu'un rapport est nécessaire pour chaque transfert, mais on ne saurait exclure la possibilité, lorsque plusieurs transferts ont lieu sous des conditions identiques vers un même pays, de ne soumettre à la Commission nationale qu'un seul rapport regroupant l'ensemble de ces transferts. Ceci permettra d'éviter des lourdeurs bureaucratiques, que la loi a justement voulu éviter, tout en se conformant au souhait du législateur.

13-76. Ensuite, un transfert ou un ensemble de transferts vers un pays tiers n'assurant pas une protection adéquate peut aussi être autorisé par la Commission nationale « 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 »[91].

Cette modalité de transfert peut s'avérer plus adaptée aux exigences du commerce international que le recours aux conditions de légitimation de l'article 19, paragraphe (1).

En effet, la Commission européenne a adopté des décisions établissant des clauses types afin de simplifier la procédure de ceux qui souhaitent exporter des données vers un pays tiers tout en voulant s'assurer d'un niveau de protection le plus élevé possible. Ces clauses types concernent soit le transfert vers un responsable du traitement établi dans un pays tiers[92], soit vers un sous-traitant établi dans un tel pays[93].

Si ces clauses ne sont pas obligatoires, il s'agit néanmoins d'un instrument qui s'avérera extrêmement utile pour opérer en toute sécurité des transferts de données vers des pays tiers. Lorsque le responsable du traitement utilise ces clauses types, la Commission nationale ne pourra pas s'opposer au transfert de données.

Le groupe d'experts institué par l'article 29 de la directive 95/46/CE a publié le 3 juin 2003 un document de travail traitant de la possibilité pour les sociétés multinationales d'adopter des codes de conduite relatifs aux transferts intragroupes de données[94].

Ces codes de conduite constituent une manière de concilier les exigences de la protection des personnes concernées en cas de transfert de leurs données avec les contraintes du commerce international et des réseaux de télécommunications.

La Commission européenne a d'ailleurs reconnu l'obligation de « travailler davantage à la simplification des conditions des transferts internationaux »[95].

Afin d'assurer le respect des conditions du traitement et des droits de la personne concernée, la loi a mis en place différents mécanismes de contrôle et de surveillance qui se veulent efficaces tout en restant proches des préoccupations du responsable du traitement.

[91] Article 19, paragraphe (3), de la loi.

[92] Décision de la Commission 2001/497/CE du 15 juin 2001 ; *J.O.C.E.* L 181/19.

[93] Décision de la Commission 2002/16/CE du 27 décembre 2001, *J.O.C.E.* L 6/52.

[94] Document de travail WP74, disponible sur : www.europa.eu.int/comm/privacy

[95] Premier rapport de la Commission européenne sur la mise en œuvre de la directive relative à la protection des données adopté le 15 mai 2003 COM (2003) 265 final, p.22.

TITRE V

Les mécanismes de contrôle et de recours

13-77. Une loi qui entend établir un équilibre, certes délicat, entre les intérêts du responsable du traitement et les droits et libertés fondamentaux de la personne concernée, doit comporter des mécanismes de contrôle et de recours efficaces. Il s'agit d'éviter que ne se réitère l'expérience malheureuse de la commission consultative instituée par la loi du 31 mars 1979, qui fut rapidement dans l'incapacité de faire face à sa tâche à tel point qu'il s'en suivit une paralysie complète du système.
La loi prévoit ainsi un mécanisme de contrôle tant externe par la Commission nationale qu'interne par le biais du chargé de la protection des données et des mesures de sécurité (chapitre 1). Un tel contrôle ne suffit cependant pas et des recours administratifs et juridictionnels sont prévus par la loi (chapitre 2).

CHAPITRE 1

Les mécanismes de contrôle

13-78. Le contrôle des traitements est l'œuvre de la Commission nationale (section 1) et du chargé de la protection des données (section 2). En outre, le responsable du traitement doit prendre un certain nombre de mesures de sécurité (section 3).

SECTION 1

La Commission nationale pour la protection des données

13-79. La Commission nationale est un établissement public dont le siège est à Esch-sur-Alzette. Elle est composée de trois membres effectifs et de trois membres suppléants, nommés par le Grand-Duc sur proposition du gouvernement en conseil pour un terme de six ans renouvelable une fois. La Commission nationale est un organe indépendant[96].

13-80. Conformément à l'article 32, paragraphe (1), de la loi, la Commission nationale 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 ».
Parmi les nombreuses missions énumérées à cet article 32 figurent les autorisations que la Commission nationale doit délivrer pour les traitements visés à

[96] Article 34, paragraphe (1), alinéa 3, et article 35, paragraphe (8), de la loi.

l'article 14 et les notifications qu'elle doit recevoir pour les autres traitements ainsi que la tenue du registre public comprenant les autorisations et les notifications.
Toute personne concernée peut saisir la Commission nationale afin de faire respecter ses droits et libertés fondamentaux. Le silence gardé par la Commission nationale pendant une durée de trois mois (ou, pour les cas visés par l'article 11, un mois[97]) à compter de sa saisine, vaut décision implicite de rejet.
Afin d'être en mesure de remplir sa mission, la Commission nationale dispose d'un droit d'investigation pour contrôler la licéité et la légitimité d'un traitement. Elle peut même procéder à des vérifications sur place sans que ni le chargé de la protection des données ni le prestataire de services de certification ne puissent lui opposer le secret professionnel auquel ils sont soumis[98].
La Commission nationale a le droit d'ester en justice et peut intenter dans les conditions de l'article 39 une action en cessation[99]. Elle a l'obligation de dénoncer aux autorités judiciaires les infractions à la loi afin de permettre à ces autorités de déclencher l'action publique ou une action en cessation.

13-81. La Commission nationale dispose également d'un pouvoir disciplinaire visé à l'article 33 de la loi. Les sanctions disciplinaires comprennent l'avertissement ou l'admonestation du responsable du traitement qui a méconnu les dispositions de la loi concernant la subordination et la sécurité des traitements[100], le verrouillage, l'effacement ou la destruction des données traitées de manière contraire à la loi ainsi que l'interdiction temporaire ou définitive d'un traitement illégal. La décision de la Commission nationale peut faire l'objet d'une publication aux frais de la personne sanctionnée. Celle-ci peut intenter un recours en réformation devant les juridictions administratives contre une sanction disciplinaire prononcée à son encontre.
En complément de la surveillance opérée par la Commission nationale, la loi a innové en prévoyant l'institution d'un chargé de la protection des données responsable de la surveillance de certains traitements.

SECTION 2
Le chargé de la protection des données

13-82. Le chargé de la protection des données est une personne physique ou morale chargée par le responsable du traitement de contrôler si les traitements

[97] L'article 11 traite de la surveillance sur le lieu du travail.
[98] À savoir l'article 24 de la loi en ce qui concerne le chargé de la protection des données et l'article 19 de la loi du 14 août 2000 relative au commerce électronique pour le prestataire de services de certification.
[99] Voy. chapitre 2 ci-après.
[100] Articles 21 à 24 de la loi.

mis en œuvre sont conformes aux dispositions de la loi. Il dispose d'un pouvoir d'investigation et d'un droit d'information auprès du responsable du traitement. Il a également le droit d'informer le responsable du traitement des mesures à prendre pour se conformer à la loi. Le chargé de la protection des données peut interroger la Commission nationale en cas de doute[101].
La nomination d'un chargé de la protection des données n'est cependant pas une obligation pour le responsable du traitement. « 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 » »[102].
Le chargé de la protection des données ne peut contrôler que des traitements qui doivent être notifiés à la Commission nationale. Il lui est interdit de surveiller des traitements qui, en application de l'article 14 de la loi, doivent être autorisés par la Commission nationale. En effet, dans la mesure où les traitements confiés à la surveillance d'un chargé de la protection des données ne doivent plus être notifiés à la Commission nationale, le charger également des traitements soumis à autorisation reviendrait à lui donner un pouvoir d'autorisation, c'est-à-dire de prendre des décisions administratives[103].
L'article 12, paragraphe (3), lettre (a), de la loi fait obligation au chargé de la protection des données de tenir un registre des traitements soumis à sa surveillance. Ce registre est notifié à la Commission nationale afin de lui permettre d'exercer, si besoin en était, son pouvoir de contrôle et d'investigation. Les traitements surveillés par le chargé de la protection des données figurent également sur le registre public prévu à l'article 15 de la loi.

13-83. Le responsable du traitement informe la Commission nationale de la désignation d'un chargé de la protection des données et lui communique son identité. Un tel chargé de la protection des données doit satisfaire à un certain nombre de critères.
D'abord, il doit être indépendant vis-à-vis du responsable du traitement. Il ne doit exister ni lien de subordination ni contrat de travail entre le responsable du traitement et le chargé de la protection des données. La révocation du chargé de la protection des données par le responsable du traitement ne peut intervenir qu'en cas de violation de ses obligations légales ou conventionnelles[104].

[101] Article 40, paragraphe (4).
[102] *Doc. parl.* 4735-13, p. 38.
[103] *Doc. parl.* 4735, p. 50.
[104] Article 40, paragraphe (3), lettre (b).

Ensuite, le chargé de la protection des données doit être agréé par la Commission nationale. Il doit justifier avoir accompli une formation universitaire en droit, économie, gestion d'entreprise, sciences de la nature ou informatique et disposer d'assises financières de vingt mille euros. Cependant, les membres de certaines professions réglementées n'ont pas besoin de remplir la condition de l'assise financière. Il s'agit des avocats à la Cour, des réviseurs d'entreprises, des experts-comptables et des médecins, cette liste pouvant être complétée par règlement grand-ducal.

La Commission nationale peut s'opposer à tout moment à la désignation d'un chargé de la protection des données 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 »[105].

Il n'y a pas de durée maximale pour exercer les fonctions de chargé de la protection des données, mais celui-ci peut être soumis à un contrôle continu de ses connaissances.

Le mandat de chargé de la protection des données n'est certainement pas à prendre à la légère, car il implique une responsabilité certaine dans l'exécution d'une mission qui peut parfois s'avérer complexe.

SECTION 3
Les mesures de sécurité

13-84. « 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 »[106].

Le responsable du traitement communique les mesures de sécurité qu'il a mises en place à la Commission nationale lors de la notification du traitement ou dans le cadre de la demande d'autorisation. Le responsable du traitement doit aussi soumettre à la Commission nationale un rapport annuel sur ces mesures de sécurité.

Les mesures de sécurité doivent être respectées non seulement par le responsable du traitement et son personnel, mais également par toute personne qui agit

[105] Article 40, paragraphe (8).
[106] Article 22, paragraphe (1), de la loi.

sous son autorité, y compris donc le sous-traitant choisi par le responsable du traitement[107].
Le sous-traitant doit avoir conclu par écrit un contrat avec le responsable du traitement ou un autre acte juridique, comme un engagement unilatéral ou autre lettre de reconnaissance, dans lequel il est clairement stipulé, d'une part, que, conformément à l'article 21 de la loi, 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.
Parmi les mesures de sécurité à mettre en place, figurent les contrôles énumérés à l'article 23 de la loi. 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 [de la loi] et, en général, de la *ratio legis* de l'ensemble [de la loi] »[108].
Tout comme les mesures de contrôle, les recours juridictionnels organisés par la loi se caractérisent à la fois par leur force dissuasive et par leur caractère réaliste.

CHAPITRE 2
Les recours juridictionnels

13-85. L'intervention des juridictions en matière de protection des données s'illustre de plusieurs façons.
D'abord, les juridictions administratives peuvent être saisies d'un recours contre une décision, comme une sanction disciplinaire, prise par la Commission nationale.
Ensuite, le juge répressif peut être saisi en cas d'infraction à une disposition de la loi sanctionnée pénalement.
Puis, la personne concernée, ou toute autre personne ayant un intérêt, peut intenter une action au fond en responsabilité contractuelle ou quasi délictuelle contre le responsable du traitement.

13-86. Enfin, l'article 39 de la loi organise une action en cessation d'un traitement qui contrevient à la loi. Cette action a de fortes similitudes avec l'action en cessation prévue en matière de concurrence déloyale par l'article 21 de la loi

[107] Article 22, paragraphe (2), de la loi.
[108] *Doc. parl.* 4735-13, p. 3 7.

du 27 novembre 1986. L'action en cessation de l'article 39 de la loi n'exclut nullement la possibilité d'intenter une action en responsabilité, ces deux actions pouvant être intentées cumulativement.

L'action en cessation relève de la compétence du président du tribunal d'arrondissement du lieu du traitement. Le projet de loi initial prévoyait que l'action devait être portée devant la chambre du conseil du tribunal du lieu du traitement. Dans la mesure où les droits en jeu sont essentiellement de nature civile, le législateur a considéré que la chambre du conseil n'était pas la juridiction appropriée et lui a substitué la juridiction du président du tribunal d'arrondissement.

L'action en cessation peut être introduite soit par le procureur d'État, soit par la Commission nationale, soit encore par la personne concernée.

Le procureur d'État peut intenter une action en cessation lorsqu'une action publique pour violation de la loi a été déclenchée. L'action en cessation est indépendante de l'action publique. La suspension ou la fermeture provisoire, qui peut être ordonnée dans le cadre d'une action en cessation, prend cependant automatiquement fin en cas d'acquittement du responsable du traitement ou deux ans à compter du prononcé de la mesure provisoire au cas où aucune décision sur l'action publique n'est pas intervenue entre-temps[109].

Le président du tribunal d'arrondissement peut aussi être saisi par la Commission nationale dans l'hypothèse où le responsable du traitement n'a pas respecté une sanction disciplinaire, lorsque cette sanction a été confirmée en dernière instance par les juridictions administratives ou lorsqu'elle n'a pas fait l'objet d'un recours.

Le droit de saisine appartient encore à la personne concernée. Sous peine d'irrecevabilité, la personne concernée doit cependant passer par le filtre de la Commission nationale. Elle doit d'abord saisir la Commission nationale et ce n'est qu'en cas d'inaction de celle-ci ou en cas de décision de rejet prise par cet établissement public que la personne concernée peut intenter une action en cessation.

L'action en cessation est recevable « même lorsque le traitement illégal a pris fin ou n'est plus susceptible de se reproduire ». Cette précision figurant au paragraphe (2) de l'article 39 est reprise de la jurisprudence intervenue au sujet de l'action en cessation en matière de concurrence déloyale[110].

Le président du tribunal d'arrondissement *doit* ordonner la cessation de tout traitement contraire aux prescriptions de la loi et la suspension provisoire de l'activité du responsable du traitement ou du sous-traitant. En outre, il *peut* ordonner la fermeture provisoire de l'établissement du responsable du traitement ou du sous-traitant lorsque la seule activité de l'un ou de l'autre consiste dans le traitement de données. Peu importe, dans cette dernière hypothèse, que

[109] Article 39, paragraphe (6), de la loi.

[110] Cour, 31 mai 1978, *Pas.*, 24, p. 127.

le sous-traitant effectue également des traitements pour d'autres responsables du traitement[111]. Mais le sous-traitant ne peut se voir sanctionné que si une infraction à la loi lui est personnellement imputable. Le président peut assortir la cessation d'une astreinte[112]. Le paragraphe (5) de l'article 39 prévoit également la possibilité de faire publier, aux frais de la personne sanctionnée, la décision de cessation dans des journaux ou de toute autre manière, par exemple sur un site Internet, à condition que la condamnation soit coulée en force de chose jugée.

L'action est introduite comme en matière de référé et, à l'instar de la loi du 27 novembre 1986, la voie de recours de l'opposition est exclue.

Cette action en cessation constitue un moyen efficace et rapide pour sanctionner le responsable du traitement qui contreviendrait aux prescriptions de la loi et pour protéger les droits de la personne concernée.

Conclusion

13-87. La loi du 2 août 2002 constitue sans nul doute un progrès significatif[113] par rapport à la loi du 31 mars 1979. Son but est d'instituer un équilibre entre les intérêts du responsable du traitement et les droits de la personne concernée. Une balance des intérêts de la personne concernée et du responsable du traitement n'est pas aisée à obtenir. Elle est encore plus difficile à conserver à la longue. Mais, à aucun moment, cette balance ne doit durablement pencher de l'un comme de l'autre côté puisque, alors, le but recherché au niveau communautaire et au niveau national aura définitivement été manqué et le gâchis sera consommé.

Sans vouloir s'enfermer dans un carcan théorique, il semble que la loi avait l'ambition d'être réaliste et proche des préoccupations de tous ceux qui doivent traiter des données dans le cadre de leur profession. La pratique montrera si cette ambition est réalisée[114].

Les acteurs de la place financière n'échapperont que très rarement à l'emprise de la loi et devront y adapter leurs procédures et mécanismes internes. Sans être révolutionnaire, puisque les obligations imposées par la loi du 31 mars 1979 étaient beaucoup plus lourdes[115] et rigides, la loi constitue la prise en compte des droits de la personne concernée.

[111] *Doc. parl.* 4735-13, p. 41.
[112] Article 39, paragraphe (4), de la loi.
[113] Même s'il s'avère que la loi, dans certains aspects, va très loin, voire trop loin.
[114] En prenant en compte certains défauts de jeunesse qu'il conviendra de rectifier.
[115] Bien qu'en pratique cette loi fût restée lettre morte.

Il est certainement vrai que la protection des données doit être prise au sérieux. L'adaptation des procédures internes ou des documents contractuels, des nouvelles procédures administratives ne constituent qu'un des aspects de la mise en œuvre de la loi. Mais il ne faut pas se limiter à ces aspects plutôt négatifs, coûteux et chronophages. Les codes de conduite sectoriels ou intragroupes devront permettre la mise en place de mécanismes de traitement de données sûrs et pratiques. L'attitude des autorités devra être réaliste et proche des préoccupations des uns comme des autres, même si ce ne sera pas sans poser des difficultés par moment.

Mais une fois les incertitudes balayées et les écueils levés, il peut être espéré que la loi sera un outil indispensable pour guider le comportement des responsables du traitement ainsi que des personnes concernées.