N° 5554[2]

CHAMBRE DES DEPUTES

Session ordinaire 2006-2007

PROJET DE LOI

portant modification

- **de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel;**
- **des articles 5 paragraphe (1) lettre a); 9 paragraphe (1) lettre a) et 12 de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et**
- **de l'article 23 paragraphe (2) points 1. et 2. de la loi du 8 juin 2004 sur la liberté d'expression dans les médias**

* * *

AVIS DE LA CHAMBRE DE TRAVAIL

(29.9.2006)

Par lettre en date du 29 mars 2006, notre chambre a été saisie pour avis du projet de loi portant modification 1. de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel; 2. des articles 5 paragraphe (1) lettre a), 9 paragraphe (1) lettre a) et 12 de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et 3. de l'article 23 paragraphe (2) points 1. et 2. de la loi du 8 juin 2004 sur la liberté d'expression dans les médias.

Même si elle approuve *in globo* la simplification des formalités administratives prévue à l'article 12, notre chambre, à l'instar de son avis 54/2000 rendu en date du 14 novembre 2001 concernant le projet de loi No 4537 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel, ne peut approuver le projet de loi pour les motifs suivants:

*

I. LES LIBERTES INDIVIDUELLES GRAVEMENT MENACEES

1. L'absence de réglementation universelle et coercitive en ce qui concerne la protection des personnes à l'égard du traitement des données à caractère personnel met en cause l'efficacité de la directive 95/46/CE ainsi que sa transposition dans la législation nationale des Etats membres!

S'il est légitime et nécessaire de protéger les valeurs fondamentales de la société surtout lorsqu'elles ont des finalités diamétralement opposées telles la libre circulation des données à caractère personnel, d'une part, et les libertés individuelles, d'autre part, il est, malgré tout, sinon absurde du moins douteux de ne soumettre qu'une partie de la communauté internationale à des règles contraignantes – telle l'Union européenne – et de laisser au reste des pays d'en juger à leur gré.

Cet état des choses est contraire au principe de la réciprocité, principe sacrosaint en matière de droit international.

Même si l'Union européenne s'est donné un cadre juridique pour essayer de concilier la libre circulation des données à caractère personnel (principe fondamental du traité de Rome) et les libertés individuelles du citoyen – tel le droit à la vie privée[1] - (assurées par la Convention européenne des droits de l'Homme), toujours est-il que le traitement de données à caractère personnel exigé par les autorités d'un pays tiers à l'Union européenne n'est pas soumis à la directive. Outre le fait que les pays tiers ne sont pas soumis à la directive, certains exigent de la part des pays de l'Union européenne le transfert de données à caractère personnel sous peine d'appliquer des sanctions économiques et politiques.

Ainsi, les Etats-Unis viennent d'imposer aux compagnies aériennes de leur céder la quasi-totalité des données fournies par les passagers dans les vols transatlantiques, ceci au mépris de ladite directive. Le chantage était clair: ou bien les données, ou bien une amende pouvant aller jusqu'à 5.400 € par passager, voire carrément l'interdiction d'atterrissage aux Etats-Unis. Désormais, les Etats-Unis ont accès à la grande majorité des quarante données contenues dans le dossier du passager, le fameux PNR (Passenger Name Record): moyen de paiement, numéro de siège, contact sur place, nombre de personnes voyageant ensemble, santé du passager, régime alimentaire, réservation d'hôtel etc.

Outre l'atteinte aux libertés individuelles, cet abandon entraîne de lourdes conséquences économiques. Qui peut garantir que ces informations ne seront jamais utilisées dans le dessein de retracer et d'analyser les déplacements des cadres importants et des dirigeants d'entreprise dans le cadre des grandes compétitions commerciales internationales? Personne. C'est bien un formidable outil d'intelligence économique que l'Europe livre aux Américains. Sans aucune réciprocité entre les deux continents.

Il en va de même pour le transport maritime où les Etats-Unis ont obligé les grands ports à travers le monde à se soumettre à leurs exigences.

Ainsi des douaniers américains inspectent tous les jours les navires dans les ports du Havre et de Marseille alors que les fonctionnaires du ministère des Transports français en vertu de la réglementation nationale et européenne n'ont pas un accès libre aux installations portuaires.

L'absence de réglementation internationale en ce qui concerne la protection des personnes à l'égard du traitement de données à caractère personnel rend superflue voire même contre-productive une législation – telles la directive et les législations nationales des Etats membres ayant transposé cette directive – qui ne s'impose qu'à une partie de la Communauté internationale.

Nul n'ignore que dans des pays tiers à l'Union européenne, on peut capter par des moyens techniques de plus en plus sophistiqués, à des fins d'espionnage économique et militaire, sans pour autant que l'auteur se voie infliger des sanctions, toutes sortes de données à caractère personnel tombant sous le champ d'application de la directive.

2. La lutte contre le terrorisme, un faux-fuyant pour éluder le respect des droits fondamentaux du citoyen et pour éclore un marché financièrement alléchant!

2.1. *La lutte contre le terrorisme, un faux-fuyant pour éluder le respect des droits fondamentaux!*

Après les attentats meurtriers du 11 septembre 2001 au WTC à New-York et au Pentagone à Washington, ceux de Madrid en 2004 et de Londres en 2005, la voie empruntée par la plupart des Etats de la Communauté internationale était de renforcer le dispositif sécuritaire par une technoconcentration de moyens (installation tentaculaire de caméras et d'autres dispositifs de vidéo-surveillance à des endroits dits, selon l'article 10 du projet de loi, *lieux à risque*, surveillance de l'utilisation des ressources informatiques par des procédés de plus en plus sophistiqués, écoutes téléphoniques, introduction de

---

1 Article 8 de la Convention européenne des droits de l'homme

„1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui."

passeports biométriques, la constitution d'une banque de données génétiques à des fins de procédures d'enquête préliminaire par le Procureur d'Etat ou la police) ayant pour objet, dit-on, de sauvegarder nos sociétés démocratiques de l'axe du Mal.

En raison de cette prolifération des moyens de surveillance, le citoyen risque de devenir un „terroriste potentiel" aux yeux des autorités publiques. Or, le principe dans un Etat de Droit devrait être que ce n'est pas au citoyen de se justifier auprès des autorités publiques, mais, au contraire que, c'est à celles-ci de prouver le bien-fondé des mesures destinées à restreindre les libertés individuelles comme l'installation de moyens de surveillance[2].

Notre chambre tient à renvoyer à son avis 30/2002 concernant le projet de loi portant 1) répression du terrorisme et de son financement 2) approbation de la Convention internationale pour la répression du financement du terrorisme, ouverte à la signature à New-York en date du 10 janvier 2000, dans lequel elle a soulevé le caractère équivoque de la notion de terrorisme[3].

Le prétexte de la lutte contre le terrorisme ne permet pas seulement aux pays tiers de l'Union européenne de ménager le traitement de données à caractère personnel comme bon leur semble (voir point 1), mais également aux Etats membres de l'Union européenne d'entraver les libertés individuelles du citoyen par une ribambelle de dispositions prévues tant dans la directive que dans leur législation nationale permettant d'entraver les droits fondamentaux du citoyen comme le droit à la vie privée, réduit au fil des dernières décennies à son plus petit dénominateur commun.

Bien que la lutte contre le terrorisme ne fasse *expressis verbis* partie intégrante du projet de loi en cause, elle constitue néanmoins le justificatif inofficiel pour introduire toute une série de dispositions permettant aux autorités publiques de recueillir des informations à caractère personnel dans le cadre de la prévention, de la recherche et de la constatation des infractions pénales et notamment dans l'hypothèse où la sûreté de l'Etat, la défense et la sécurité publique le requièrent.

A l'instar de ce qu'elle a déjà soulevé dans son avis 54/2000, notre chambre ne peut que soulever l'inefficacité tant de la loi du 2 août 2002 précitée que du projet de loi en cause qui brillent par une kyrielle d'exceptions aux principes d'interdiction de traitement de données à caractère personnel et aux droits fondamentaux si solennellement évoqués dans l'exposé des motifs que tout lecteur vient forcément à la conclusion que les droits fondamentaux de la personne (surtout le droit à la vie privée) sont réduits à la portion congrue.

Prenons quelques exemples à titre d'illustrations.

Tandis que l'article 6 interdit dans son premier paragraphe *les traitements qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les traitements de données génétiques*, les deuxième et troisième paragraphes énumèrent bel et bien quatorze exceptions où cette interdiction est levée, notamment en ce qui concerne les données génétiques (paragraphe 3, point a), *pour vérifier l'existence d'un lien génétique dans le cadre de l'administration de la preuve en justice pour l'identification d'une personne, la prévention ou la répression d'une infraction pénale déterminée dans les cas visés au paragraphe (2) du présent article par les lettres (f), (h) et (i).*

Si notre chambre ne nie pas l'intérêt en tant que tel de traiter des données génétiques dans certains cas limitativement énumérés, elle s'oppose toutefois au champ d'application beaucoup trop vaste et flou dans lequel de telles données peuvent être traitées.

L'article 6(3) a) permet ainsi au ministère public et au juge d'instruction d'ordonner par exemple une analyse ADN sans préciser à quel moment, dans quelles conditions et surtout pour quel genre d'infractions un traitement de données génétiques est possible.

De plus, le texte ne souffle mot sur les personnes qui peuvent faire l'objet d'un tel traitement. Ceci est laissé à l'appréciation arbitraire du ministère public et du juge d'instruction qui non seulement

---

2 Die Zeit 41/2001 „Datenschutz = Terroristenschutz? Unsinn!" (…) „Es gibt keine demokratische Gesellschaft, die nicht risikobehaftet ist. Wir müssen uns mit dem Terrorismus auseinander setzen und neue Wege beschreiten. Aber das darf doch nicht heissen, dass wir in diesem Kampf all unsere Grundsätze preisgeben, sonst hätten am Ende die Terroristen über uns gesiegt.

Grundsätze, dass der Staat in einem Gesetz begründet und beweispflichtig ist, wann, von wem und zu welchem Zweck er Daten braucht. Dass er die Betroffenen zu einem geeigneten Zeitpunkt davon in Kenntnis setzt. Und dass er die Daten niemals auf Vorrat sammeln darf. Denn solch ein Vorrat hat eine fatale Folge: er bleibt auf immer und ewig bestehen."

3 Monde diplomatique février 2004 „Qu'est-ce que le terrorisme?" Par Jacques DERRIDA, philosophe et écrivain.

tendent à éclaircir sur des faits pénalement sanctionnés par la loi, mais qui, en même temps, jugent eux-mêmes du bien-fondé de leurs propres actes.

Ils gèrent et contrôlent les banques de données génétiques dans le cadre de la procédure pénale, à l'exclusion de toute autre instance impartiale comme p. ex. la CNPD[4].

Une telle ouverture viole sans aucun doute le principe de finalité et de proportionnalité du traitement des données génétiques et transgresse les libertés individuelles du citoyen parmi lesquelles il y a lieu de soulever avant tout le droit à la vie privée.

Un autre domaine sensible dans lequel le principe de proportionnalité et de finalité sont bafoués est celui de l'article 17 du projet de loi ainsi que celui des articles 88-1 à 88-4 du Code d'instruction criminelle concernant les mesures spéciales de surveillance (comme p. ex. l'enregistrement d'entretiens téléphoniques et les écoutes téléphoniques).

En confrontant les articles 6(1) aux articles 6(2) et 17, on n'arrive plus à déceler ce qui est „principe" et ce qui est „dérogation". La confusion est telle que notre chambre craint que l'article 17 qui autorise *des traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions* ne prime sur le principe d'interdiction de traitement des données sensibles prévu à l'article 6(1). En effet le texte de l'article 17 est libellé dans des termes si flous que les autorités chargées de la détection des infractions ont main libre pour ordonner des traitements de toute nature pour TOUT genre d'infraction.

Dans ce contexte, notre chambre tient à réitérer son inquiétude à l'égard des droits de la défense et de l'existence d'une voie de recours judiciaire effective. Notre chambre tient à souligner que, dans le cadre de l'article 17, le droit à l'information de la personne concernée ainsi que le droit d'accès aux informations ne jouent pas du tout ou ne jouent que de façon restrictive (voir articles 27 et 29).

Ainsi l'article 17 du projet de loi permet-il à un règlement grand-ducal de déroger au principe d'interdiction de traitement de catégories particulières de données conformément à l'article 6(2) h) et donc d'échapper aux sanctions pénales prévues à l'article 6(5). En d'autres mots, le pouvoir exécutif peut décider de façon arbitraire sans devoir recueillir l'approbation du parlement quels traitements échappent au principe d'interdiction de traitement de catégories particulières de données. Autrement dit, l'Etat contrôle lui-même ses propres actes, ce qui est contraire au principe de la séparation des pouvoirs et à l'essence même de l'Etat de Droit.

2.2. *La lutte contre le terrorisme, un faux-fuyant pour éclore un marché financièrement alléchant!*

Etant donné que depuis les attentats au WTC à New York en 2001, la lutte contre le terrorisme est restée l'apanage de la politique des Etats-Unis qui, jusqu'à présent, ont menacé ou attaqué tout pays, tout peuple dont ils estiment qu'ils sont à l'origine des agressions lancées contre leur propre pays (même si le chef du réseau terroriste d'Al Khaida, Oussama Bin Laden, persona non grata en Arabie-Saoudite, s'est réfugié en Afghanistan et n'est pas identifiable en tant que tel avec le peuple afghanistanais), quiconque doit conclure que *„les opérations militaires et ingérences humanitaires"* des Etats-Unis et de certains de ses alliés (ne parlons surtout pas de guerre!), bref, la lutte contre le terrorisme (ce fantôme non identifié!) ne constitue pas une fin en soi, mais un moyen pour renforcer les intérêts de ceux-ci dans le monde, avant tout les intérêts économiques.

Au lieu de réviser leur propre politique étrangère à l'égard des pays suspectés de soutenir le terrorisme, la plupart des pays du pacte atlantique ont procédé à un renforcement du dispositif sécuritaire en ne visant plus seulement les auteurs des attentats de New York, Madrid, Londres ou autres, mais également un grand nombre d'étrangers considérés, pour des raisons indépendantes du terrorisme, comme „indésirables", ainsi que l'ensemble des populations.

Les attentats précités donnèrent lieu à une surenchère de dispositifs visant à accumuler un savoir précis sur des millions de personnes, afin d'en extraire des renseignements sur la potentielle malfaisance de *quelques* individus.

Ainsi a-t-on procédé à radiographier les voyageurs et le contenu de leurs bagages, à stocker des données biométriques, à surveiller les portables, à archiver des myriades de numéros de téléphone, à numériser les empreintes digitales, à croiser les fichiers géants d'administrations ou d'entreprises.

---

4 Letzebuerger Land du 14 avril 2006 „Riskante Wunderwaffe"

Pourquoi les Londoniens sont-ils contraints à se faire photographier 300 fois par jour, à se faire filmer continuellement avec 2,5 millions de caméras disséminées alors qu'on sait très bien que cela n'a pas empêché les terroristes de déclencher leurs bombes le 7 juillet 2005?

Au-delà des prétextes de maintien de l'ordre, il n'existe qu'une explication pertinente: les institutions et les entreprises découvrent dans la gestion de la peur un gisement durable de pouvoir, de contrôle et de profit.

Depuis le 11 septembre 2001, la politique des Etats-Unis et de ses alliés consiste à remobiliser la planète entière autour de l'objectif sécuritaire.

Quatre mouvements intriqués structurent cette mutation:

– une accélération des connexions entre innovations dans différents segments du marché de la peur: identification, surveillance, protection, arrestation, détention;
– une fusion entre reconversion des industries de guerre et des organisations militaires dans la formation et l'équipement de forces répressives, et militarisation concomitante des forces de sécurité civile;
– une articulation grandissante entre puissances publiques et puissances privées, tant en matière de contrôle des identités que de capacité à contraindre et interdire;
– une poussée idéologique, conjointement menée dans les domaines juridique, politique, administratif, économique et médiatique, visant à pérenniser l'angoisse „sécurisable" et à faire accepter le contrôle préventif généralisé comme nouvelle normalité de l'existence humaine.

Quelques exemples, au hasard. En France, une filiale de TF1, Visiowave, use de ses compétences télévisuelles pour détecter les comportements suspects sur les lieux publics (grâce à des logiciels d'interprétation des gestes) et produire des publireportages sur les écrans de métro et de bus. Thales (ex-Thomson CSF) produit des panoplies de surveillance, sans hésiter à les vendre à des Etats autoritaires. Les grands de l'informatique et de l'électronique ne sont pas en reste, tels Microsoft et sa fameuse puce Palladium, capable de contrôler, de l'extérieur, la gestion des fichiers des PC, ou Sony, qui pense diffuser dans le monde entier, pour un chiffre d'affaires estimé à 3 milliards de dollars en 2009, son étiquette „sans contact", détectable par radiofréquence (RFID) et apte à traquer des produits marqués au domicile de leurs acheteurs … ou de leurs voleurs!

Après ce déploiement technologique préparant la „société de contrôle", le second trait frappant de ce nouveau capitalisme réside dans la fusion progressive entre la peur de l'ennemi et la défiance envers le citoyen, entre le militaire et le policier. Le phénomène atteint la plupart des pays occidentaux, qui réorientent en partie leur course aux armements vers l'escalade de sécurité civile.

Au vu des développements ci-dessus, notre chambre ne peut que constater la consécration des droits fondamentaux de l'homme au profit de la libre circulation des données à caractère personnel, constat que notre chambre a déjà établi dans son avis initial 54/2000 sur le projet de loi sus-énoncé.

Elle ne saura par conséquent approuver le projet de loi qui n'est rien d'autre qu'un trompe-l'oeil et un désastre pour les libertés individuelles.

Ce n'est qu'à titre subsidiaire et pour les besoins de la cause, que notre chambre procède à l'analyse du projet de loi proprement dit.

Pour ce faire, elle reprend les remarques de son avis initial 54/2000 pour autant que celles-ci gardent leur pertinence tout en prenant en compte des modifications de texte proposées par le présent projet de loi.

*

II. UN PROJET DE LOI INDIGESTE, ILLISIBLE ET INAPPLICABLE

A l'instar de son avis 54/2000 concernant le projet de loi initial et du point I du présent avis, notre chambre conclut à l'inapplicabilité du présent texte de loi dans lequel on n'arrive plus à discerner le principe de l'exception, tantôt le „oui, mais" se mue en „non, sauf" et vice-versa.

De plus, elle opine que les deux principes sacrosaints qui constituent la trame du présent projet, le principe de finalité et le principe de proportionnalité, ne sont pas toujours garantis.

Le premier principe repose sur le postulat que la menace pour la vie privée que constituent les traitements de données à caractère personnel réside davantage dans la finalité qu'ils poursuivent que dans la nature des données traitées.

Le second précise que les données doivent être nécessaires, et non seulement utiles, pour qu'un traitement puisse être accompli. Ce principe vise l'évaluation de l'opportunité d'introduire une donnée à caractère personnel dans un traitement par rapport à la finalité de ce traitement.

C'est au sujet de ces deux principes, qui constituent le fil conducteur du projet, que notre chambre adresse la majeure partie de ses critiques.

Elle va l'illustrer par la suite dans l'analyse des articles.

1. *Ad article 1: La suppression des intérêts légalement protégés des personnes morales*

Notre chambre ne peut comprendre le bien-fondé de la suppression des intérêts des personnes morales alors que dans l'exposé des motifs du projet de loi initial, elle a encore jugé utile de sauvegarder les intérêts de celles-ci notamment afin *„… de leur permettre de protéger leur image informationnelle et éviter que des décisions soient prises à l'encontre des personnes morales sur la base d'informations incorrectes, incomplètes et erronnées.“*.

Ce revirement ne convainc pas notre chambre, mais, au contraire ne fait que corroborer son raisonnement déjà étayé dans son avis 54/2000 précité en vertu duquel la libre circulation des données à caractère personnel doit primer les libertés individuelles des citoyens, sinon comment interpréter le ralliement du gouvernement à l'avis de la Chambre de commerce dans lequel celle-ci note que *„(…) le projet, du fait de son champ d'application extrêmement large qui tend à couvrir toutes les situations de traitements possibles, risque d'être tout aussi difficilement applicable que le texte actuel (loi du 31 mars 1979)“* et que *„un certain nombre de dispositions sont difficilement compatibles avec certaines activités du secteur financier“*.

On peut en conclure que la protection des libertés individuelles n'est qu'un trompe-l'oeil qui sert tout au plus à satisfaire les besoins du marché.

Plutôt que de constater qu'un certain nombre de dispositions (présumées protéger les libertés individuelles) sont incompatibles avec certaines activités du secteur financier, notre chambre se permet de poser la question par l'autre bout pour demander dans quelle mesure les activités du secteur financier sont compatibles avec les droits de l'homme.

2. *Ad article 2 p): Une définition plus restrictive de la surveillance au détriment des libertés individuelles du citoyen*

Contrairement au texte actuel, le législateur restreint la notion de surveillance dans la mesure où le traitement de données à caractère personnel opéré *de façon occasionnelle* n'est plus considéré comme surveillance. En d'autres mots, les enregistrements occasionnels ne tombent plus sous le champ d'application des articles 10 et 11 et ne sont, par conséquent, plus soumis à l'autorisation préalable de la CNPD.

Une fois de plus, le projet de loi est en retrait par rapport à la loi du 8 août 2002 et ouvre davantage la brèche aux abus, ceci au grand dam des libertés individuelles. A ce sujet, il faut se poser les questions suivantes: qu'entend-on par l'expression „occasionnelle“? Qui en décide? Comment la personne concernée faisant l'objet d'un enregistrement peut-elle en prendre connaissance pour se défendre? Notre chambre renvoie au commentaire des articles suivants.

3. *Ad article 5: Légitimité du traitement*

L'article 5 prévoit différentes conditions, en application desquelles un traitement portant sur des données à caractère personnel est considéré comme légitime.

Comme les conditions de légitimité sont alternatives et non pas cumulatives, il se peut très bien qu'un traitement remplit la condition (a), mais poserait des problèmes au niveau de la condition (d).

On pourrait ainsi imaginer que, par exemple, des écoutes téléphoniques soient légitimes sur base de la condition (a), parce qu'il existe des dispositions légales permettant sous certaines conditions de recourir à ces mesures alors qu'elles ne le seraient pas au vu de la condition (d), parce que les droits et libertés fondamentaux de la personne suspectée et de ses concitoyens seraient lésés, notamment lorsque la mesure est disproportionnée par rapport au but poursuivi ou excède la finalité initiale pour laquelle elle a été prévue.

Dans le cas en l'espèce, il pourrait y avoir un conflit entre deux conditions qui sont susceptibles de s'appliquer toutes les deux, sachant toutefois qu'elles sont alternatives.

Cela voudrait-il dire que la Commission nationale de la protection des données pourrait se baser sur la condition (a) pour éviter l'application de la condition (d) ou vice-versa?

Notre chambre est d'avis que si plusieurs conditions peuvent s'appliquer simultanément à une situation donnée, il faudra évaluer les différentes conditions entre elles. S'il se révélait qu'en vertu du principe de finalité ou de proportionnalité, le traitement excéderait sa finalité ou serait disproportionné, il devrait être interdit.

Ainsi, si dans notre cas une disposition légale prévoit de recourir sous certaines conditions aux écoutes téléphoniques, il doit rester possible de l'écarter s'il se révèle qu'elle ne remplit pas les critères de finalité et de proportionnalité tels que prévus aux articles 4 paragraphe 1(b) et 5 paragraphe 1(d).

4. *Ad article 6: Traitement de catégories particulières de données (données sensibles)*

A l'instar de ce qui a été dit sous la partie I., point 2.2., il est légitime de se poser la question de savoir si l'interdiction de traitement des données dites sensibles constitue le principe, eu égard à la multitude d'exceptions prévues par ce même article.

Même si le remaniement du paragraphe 3 énumérant les cas dans lesquels des données génétiques peuvent être traitées contribue à une meilleure lisibilité et compréhension du texte que le texte actuellement en vigueur, notre chambre craint une généralisation du traitement de ces données dans la mesure où le texte le permet *„pour vérifier l'existence d'un lien génétique dans le cadre de l'administration de la preuve en justice, pour l'identification d'une personne, la prévention ou la répression d'une infraction pénale déterminée dans les cas visés au parapraphe 2 du présent article par les lettres (f), (h) et (i)..“*.

Force est cependant de constater que 1) la nature des infractions pour lesquelles un tel traitement est autorisé n'est pas définie et 2) que le ministère public aussi bien que le juge d'instruction sont libres de juger à leur guise, sans être soumis à un contrôle quelconque, dans quelle hypothèse et à quel moment un tel traitement est ordonné. Par ailleurs, la banque de données génétiques n'est pas soumise à un contrôle impartial, à part celui du Procureur général d'Etat[5]. Le secret de l'instruction prime-t-il dans toutes les hypothèses les libertés publiques comme le droit à la vie privée?

Notre chambre craint fortement que le recours au traitement de données génétiques ne devienne une solution de facilité dans la prévention et la répression de (presque) tout genre d'infraction[6] et, par là, enfreigne le principe de proportionnalité. A ce sujet, notre chambre tient à renvoyer à son avis 30/2002 du 6 novembre 2002 concernant le projet de loi portant répression du terrorisme dans lequel elle soulève l'ambiguïté de la notion même du terrorisme qui risque de trouver application pour des faits qui constituent tout au plus une défense légitime des personnes en cause à l'égard des autorités publiques et privées[7].

Notre chambre semble déduire du nouveau paragraphe 3 de l'article 6 que les données génétiques ne peuvent plus être traitées aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail et de droit des assurances, contrairement au texte actuel. Si l'interprétation donnée par notre chambre de ce texte est exacte, elle en félicite le gouvernement alors qu'elle s'est violemment opposée au traitement de données génétiques dans les relations de travail entre le salarié et l'employeur ainsi que dans les relations entre assureur et assuré.

5. *Ad article 10: Traitement à des fins de surveillance*

Le paragraphe 1 (b) est en somme le reflèt de ce que l'auteur essaie d'éviter, à savoir le phénomène „Big brother's watching you“[8].

Notre chambre est d'avis que depuis l'entrée en vigueur de la loi du 2 août 2002, les moyens de surveillance n'ont cessé de proliférer un peu partout et la sophistication accrue de ces moyens toujours plus performants et à peine perceptibles à l'oeil nu fait qu'on ne s'en rend même plus compte. Tout prétexte semble bon pour justifier une surveillance généralisée: insécurité, délits de vitesse, vols, terrorisme, bref, un pêle-mêle de facteurs intimidants qui sont régulièrement diffusés par les médias. A force de les répéter, le public finit par y croire.

---

5 Voir article „Riskante Wunderwaffe“ au Letzebuerger Land du 14 avri12006.

6 Projet de loi 5356 relatif aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle, article 48-7.

7 Voir point 2.1.2. de l'avis 30/2002 sus-énoncé intitulé „La définition fournie par le nouvel article 135-1 du projet de loi“.

8 „Big brother sur la route“, Le Monde du 15 juin 2006, page 20.

Notre chambre se doit de constater que par rapport au texte initial du projet de loi ayant limité le traitement à des fins de surveillance aux endroits où il existe un risque rendant le traitement nécessaire à la prévention, la recherche, la constatation et la poursuite d'infractions pénales, tant le texte actuellement en vigueur que le projet de loi avisé ont étendu le champ d'application du traitement à des fins de surveillance dans la mesure où aux endroits concernés (…) il suffit que la sécurité des usagers ou la prévention des accidents rendent un tel traitement nécessaire.

Le paragraphe b) est conçu en des termes si flous et généraux que notre chambre aimerait poser la question par l'autre bout: quels sont les endroits qui, de par leur nature, leur situation, leur configuration ou leur fréquentation ne présentent pas un risque rendant le traitement nécessaire à la sécurité des usagers ou à la prévention des accidents et qui en décide?

Tout lieu public constitue en quelque sorte un risque potentiel et on voit mal où l'on pourrait fixer une limite entre les endroits qui constituent un risque et ceux qui en sont dépourvus.

Ce paragraphe en permettant donc aux autorités d'installer des vidéocameras un peu partout, comme bon leur semble, est contraire au critère de „prévisibilité" (un des critères pour juger le principe de proportionnalité)[9].

Etant donné que la sécurité des usagers et, à plus forte raison, la délinquance au sens large sont omniprésentes non seulement dans les agglomérations, mais également dans les localités de la campagne (surtout les vols avec effraction), les autorités publiques seraient obligées d'étendre le dispositif des moyens de surveillance à l'entièreté du territoire luxembourgeois afin d'éviter une inégalité de traitement consistant à prêter moins d'attention à une infraction commise en province que dans les centres-villes.

Pour garantir la sécurité des usagers (l'Etat veut-il en faire une obligation de résultat?), les autorités luxembourgeoises sont contraintes de surveiller un peu n'importe qui et n'importe où. Faudra-t-il dorénavant installer des caméras dans les cafés et restaurants pour détecter ceux qui ne respectent pas l'interdiction de fumer ou pour surveiller la nature et la quantité de boissons que consomment les clients-automobilistes? N'est-on pas en train de stigmatiser la société et de tuer la démocratie?

Est-il finalement exagéré de prétendre que les libertés individuelles des personnes sont réduites à la portion congrue?

Pour lutter contre la délinquance et la criminalité, l'auteur du projet est prêt à prendre en otage (surveiller) la société toute entière.

Notre chambre ne saura accepter une telle généralisation des moyens de surveillance où les responsables du traitement (police, entreprises) se contentent de constater les infractions à partir de leur chaise de bureau.

Dans le même ordre d'idées, notre chambre ne saura pas non plus accepter la proposition de la CNPD qui a proposé d'insérer au paragraphe 1er à la fin de l'alinéa b) le texte suivant:

„… à la protection des biens du responsable du traitement ou d'un tiers pourvu que le lieu présente de par sa nature, sa situation, sa configuration ou sa fréquentation un risque caractérisé d'acte de vandalisme ou de vol, ou …".

Ce n'est pas, comme l'indique la CNPD dans son exposé des motifs, parce que la loi est en décalage manifeste avec des pratiques largement répandues, qu'il faudra légaliser celles-ci, mais plutôt faire cesser ces pratiques consistant à se faire justice à soi-même. La motivation de la CNPD est curieuse, d'une part, parce qu'elle a toujours été très soucieuse du respect des libertés individuelles en cas de saisine d'une autorisation préalable et, d'autre part, parce qu'elle constitue un aveu d'échec de son pouvoir de contrôle et de sanction.

Notre chambre n'analyse qu'en ordre subsidiaire le paragraphe 2 qui prévoit que „les personnes concernées sont informées par des moyens appropriés tels que des panneaux de signalisation, des circulaires (…)."

A ce sujet, elle se doit cependant de constater qu'en pratique, tel n'est souvent pas le cas.

Il n'y a pas de signalisation informant le citoyen que des vidéocameras sont installées aux abords des routes ou à l'intérieur des tunnels, comme il n'y en a pas pour les vidéocameras installées (et dissimulées) à l'extérieur des établissements financiers et scolaires.

---

9 Arrêt du 30 juillet 1998 de la Cour européenne des droits de l'homme, Valenzuela Contreras c. Espagne, Recueil des arrêts et décisions 1998-V.

Par ailleurs, qu'est-ce que l'auteur entend par „personnes concernées"?

Les personnes concernées ne sont pas seulement les personnes suspectées, mais également toutes les autres personnes qui se font capter contre leur gré, faute de signalisation, par une caméra.

Dans un ordre très subsidiaire, et pour autant que le traitement à des fins de surveillance soit indispensable, quod non, notre chambre est d'avis que la signalisation de vidéocameras pourrait décourager bon nombre de délinquants potentiels à commettre des infractions, parce qu'ils n'oseraient pas exécuter leurs projets s'ils savaient que leurs actes seraient enregistrés et pourraient, le cas échéant, valoir comme moyen de preuve en justice.

6. *Ad article 11: Traitement à des fins de surveillance sur le lieu de travail*

Par nature, la caméra constitue un moyen excessivement disproportionné au but recherché par l'employeur, qu'il s'agisse de la discipline, de l'amélioration de la productivité, de la sécurité ou encore de la lutte contre les vols. L'enregistrement continu des faits et gestes du salarié dans son activité professionnelle permet, en effet, de mettre en évidence des éléments qui ne relèvent pas de la sphère professionnelle, mais ressortent de la personnalité, de l'identité de l'individu.

A ce sujet, il y a lieu de se référer à un passage d'un article du „Monde diplomatique" (août 1999) dont la teneur est la suivante:

> „ (…) Une étude menée en 1998 par l'American Management Association sur mille quatre-vingt-cinq firmes, montre ainsi que 40% des entreprises sont engagées dans une forme de surveillance intrusive de leurs employés. Elles vérifient les courriers électroniques, les conversations téléphoniques, le contenu des boîtes vocales, saisissent les mots de passe des ordinateurs individuels, enregistrent sur vidéo numérique les performances de travail. Le contrôle aléatoire de la présence de drogue dans le sang est le fait de 41% des entreprises américaines, tandis que 15% pratiquent des tests psychologiques cherchant à connaître les pensées intimes et les attitudes."

Notre chambre craint fort que de telles pratiques n'existent également au Luxembourg. Bien que la volonté du Gouvernement de légiférer en la matière soit en elle-même louable, mais qu'il existe un risque permanent de violation des droits fondamentaux dans la mise en oeuvre des moyens de surveillance, la loi sert donc tout au plus à légaliser ces pratiques, inconnues du public.

Voilà pourquoi notre chambre est d'avis que les principes de finalité et de proportionnalité des traitements des données personnelles étaient déjà voués à l'échec avant qu'ils n'aient vu le jour.

Même si un traitement à des fins de surveillance sur le lieu de travail se révélait indispensable, quod non, il serait *ab initio* impossible de l'instaurer pour une finalité limitée et déterminée, parce que le captage des images sur le lieu de travail contient inévitablement des éléments liés à l'intimité de la vie privée de chacun des travailleurs, éléments qui pourtant n'entrent pas dans la finalité initiale de la surveillance. L'impossibilité de limiter par nature la finalité du traitement entraîne par essence la disproportionnalité de cette mesure.

Ainsi le captage ou l'enregistrement d'images des travailleurs sur le lieu de travail n'entrant pas dans la finalité prévue par la loi pourraient servir comme moyen de preuve à une autre fin ou finalité.

Il se pourrait que dans le cadre de la surveillance à des fins de sécurité, une attitude ou un acte d'un salarié qui ne rentrent pas dans le champ d'application de la finalité prévue par la loi fussent utilisés ultérieurement à une autre fin, par exemple, comme moyen de preuve servant à justifier un licenciement.

Il s'agit de savoir si l'employeur peut faire valoir ce moyen de preuve illicite – car son utilisation est destinée à une finalité différente de celle prévue par la loi – pour licencier ce salarié. Le juge va-t-il admettre ce moyen de preuve en vertu du fait que „la fin justifie les moyens" ou bien va-t-il rejeter ce moyen de preuve pour cause de détournement de sa finalité?

Notre chambre s'oppose énergiquement à l'introduction de tout genre de moyens de surveillance, électroniques ou numériques, ayant notamment pour but „le contrôle temporaire de production ou des prestations du travailleur en vue de mesurer son activité afin de déterminer sa rémunération.".

Ce contrôle va rejeter le travailleur dont l'émancipation a été le fruit d'âpres luttes syndicales au terreau du prolétariat réifié du dix-neuvième siècle. Le travailleur devient de nouveau matière fongible, taillable et corvéable à merci pour les employeurs.

Notre chambre exige par ailleurs qu'un contrôle permanent doive être assuré dans les entreprises soit par l'Inspection du travail et des mines soit par la CNPD afin de vérifier que des traitements à des

fins de surveillance ne soient introduits en catimini ou en violation d'une décision de refus de la CNPD. Notre chambre craint fortement que dans la plupart des entreprises des traitements à des fins de surveillance ne soient opérés sans que personne, sauf l'employeur lui-même, s'en aperçoive. Voilà pourquoi elle revendique dans le cadre de l'article 33 que la CNPD ne doive non seulement veiller à verrouiller, effacer ou détruire les données litigieuses, mais également au démontage des moyens de surveillance ayant servi à capter des données à des fins de surveillance.

Dans un ordre très subsidiaire, et pour autant qu'un traitement à des fins de surveillance est indispensable *quod non*, notre chambre demande que le comité mixte d'entreprise doive pouvoir décider non seulement dans les cas visés aux lettres (a), (d) et (e), mais également dans les cas visés aux lettres (b) et (c), ceci conformément à la procédure qui est prévue à l'article 16 de la loi du 6 mai 1974 instituant des comités mixtes dans les entreprises. Par ailleurs, elle demande d'accorder le même pouvoir de décision aux délégués du personnel, si le comité mixte d'entreprise fait défaut.

Cet article est le corollaire de l'article 15 de la directive qui flanque le principe de protection de l'individu à l'égard de décisions individuelles automatisées prévu au paragraphe 1 de deux exceptions qui annihilent le principe prévu au paragraphe 1.

En fait, cela veut dire que si l'employeur propose au salarié au moment de la conclusion ou de l'exécution de son contrat de travail de se soumettre à un traitement à des fins de surveillance, le salarié ne peut refuser cette mesure en pratique, malgré le principe évoqué à l'article 15 paragraphe 1, s'il ne veut pas risquer de perdre son travail. Bel exemple que pratique et théorie divergent fondamentalement!

7. *Ad article 14: Autorisation préalable de la Commission*

Même si l'article 12 supprime l'obligation de notification d'un bon nombre de données à caractère personnel pour certaines finalités bien déterminées en espérant ainsi désengorger la CNPD, notre chambre reste très réservée sur les ambitions de la CNPD de (mieux) contrôler le respect de ses propres décisions rendues sur base de demandes d'autorisation préalable, compte tenu du nombre restreint de personnes actuellement à disposition.

Dans ce contexte, notre chambre se demande s'il s'agit d'une mission de contrôle générale et permanente ou uniquement d'une mission de contrôle ponctuelle se limitant aux demandes d'autorisation préalable qui ont été refusées par la CNPD.

Même si la CNPD pourrait assurer une mission de contrôle générale et permanente du point de vue de ses effectifs *quod non*, notre chambre se pose la question si un tel contrôle ne s'avérerait néanmoins inefficace dans l'hypothèse où, suite à une décision de refus ou en l'absence de décision tout court sur un traitement nécessitant une autorisation préalable de la part de la CNPD, le responsable du traitement utiliserait ou transmettrait, malgré tout, des données sensibles à un tiers qui, lui, à son tour les retransmettrait de nouveau. Notre chambre est d'avis que dans une telle hypothèse, les sanctions pénales prévues au paragraphe 7 de cet article ne sauraient ni réparer le préjudice réellement subi par la personne qui a fait l'objet d'un tel traitement ni effacer la ou les transmissions de données personnelles réellement effectuées.

8. *Ad article 17: Autorisation par voie réglementaire*

Notre chambre – à l'instar de ce qu'elle a déjà soulevé sous la partie I, point 2.1. *in fine*, s'oppose énergiquement à la façon de procéder de l'auteur qui se contente de régler le domaine du droit pénal ainsi que de la sûreté de l'Etat et de la sécurité publique par voie réglementaire, ceci pour deux raisons:

d'abord, parce que ces dispositions – d'autant plus qu'elles sont susceptibles d'affecter davantage les droits fondamentaux de la personne – devraient être intégrées dans la présente loi pour éviter que le gouvernement puisse à sa guise se tailler un règlement sur-mesure, modifiable à tout moment, qui ne nécessite pas l'approbation du parlement;

et

puis, afin que notre chambre puisse en connaissance de cause évaluer le bien-fondé de ces dispositions par rapport aux autres dispositions du projet de loi et de la directive.

9. *Ad article 18: „Principes" dans le cadre des transferts de données vers des pays tiers*

Notre chambre juge inacceptable que le texte laisse l'appréciation „du niveau adéquat de protection du pays tiers" au responsable du traitement qui, dans bien souvent des cas, a des intérêts propres dans un tel transfert. Il serait donc à la fois juge et partie.

Par ailleurs le texte ne précise nulle part ce qu'il entend par „un niveau de protection adéquat"?

Notre chambre est d'avis que le responsable du traitement doit saisir la Commission nationale de la protection des données du moment qu'il envisage de transférer des données à un pays tiers et que cette dernière doit établir des critères pour définir „le niveau de protection adéquat".

Elle ne voit pas pourquoi le texte envisage la saisine de trois acteurs différents (responsable du traitement, en cas de doute de ce dernier, la Commission nationale, sinon en cas de doute de cette dernière, la Commission européenne) pour juger le cas échéant du „niveau adéquat de protection du pays tiers". Tout cela est bien peu transparent!

En effet notre chambre se demande de quelle protection bénéficie la personne concernée si le responsable a transféré des données à un pays tiers dont le niveau de protection n'est pas „adéquat"?

10. *Ad article 19: Dérogations*

L'article 19 est tout à fait caractéristique pour tout le projet.

Il ajoute de l'arbitraire à l'arbitraire.

Cette obsession de flanquer chaque article d'une panoplie d'exceptions et de renvois rend le texte illisible, incompréhensible et partant inapplicable.

Le paragraphe 2 qui prévoit que „dans le cas d'un transfert effectué vers un pays tiers n'assurant pas un niveau de protection adéquat, le responsable du traitement doit notifier à la Commission un rapport établissant les conditions dans lesquelles il a opéré le transfert" constitue, selon notre chambre, une mesure tardive et inutile, car le transfert a déjà eu lieu et un dommage peut déjà s'être produit. On ne peut plus retourner en arrière pour effacer le transfert de traitement.

Le paragraphe 3 prévoit qu'un tel transfert peut être autorisé par la Commission même si le pays tiers n'assure pas un niveau de protection adéquat à la condition que le responsable assure des garanties suffisantes au regard de la protection des droits fondamentaux de la personne. Notre chambre doute fort que la personne concernée soit en mesure d'évaluer le bien-fondé de ces garanties afin de donner son consentement „éclairé" en toute liberté, ceci d'autant plus que le responsable du traitement a lui-même souvent des intérêts propres financiers dans un tel transfert.

La personne concernée, qui est également la partie la plus faible du point de vue économique, risque fort d'être dupée.

11. *Ad article 21: Confidentialité des traitements*

Notre chambre a de sérieux doutes qu'une manipulation, une altération ou un détournement de traitement de données ne puissent pas se faire par autrui sans l'autorisation du responsable du traitement.

Voilà pourquoi elle se demande si, et dans quelles hypothèses, la partie cocontractuelle du responsable du traitement agit vraiment „sous l'autorité du responsable du traitement".

A contrario, se pose-t-elle la question ce qu'il advient lorsque une personne n'agit pas sous l'autorité du responsable?

12. *Ad articles 22 et 23 concernant la sécurité des traitements et les mesures particulières de sécurité*

L'article montre bien que la sécurité des traitements qui incombe au responsable n'est qu'une obligation de moyens et non de résultat.

Ceci veut dire concrètement que si la personne subit un préjudice suite à une destruction, perte, altération ou diffusion de ses données, elle ne peut engager la responsabilité de l'auteur du traitement que si elle prouve une faute dans le chef de l'auteur du traitement alors que dans le cas où il se serait agi d'une obligation de résultat, la responsabilité de l'auteur du traitement aurait été établie d'office, à moins qu'il n'arrivât à s'exonérer en prouvant un cas de force majeure.

Cette atténuation de protection pour la personne concernée montre bel et bien qu'il n'existe pas de sécurité absolue en matière de traitement de données, et que tout orfèvre en la matière, que tout internaute expérimenté est en mesure de surpasser les garde-fous dans ce domaine.

Nul n'ignore que le système Echelon des Etats-Unis est apte à espionner de manière routinière téléphone, fax et courrier électronique dans le monde entier.

Compte tenu de cette réalité, plus amplement développée sous la partie I. point 1), n'est-il pas un peu osé de la part des législateurs européen et national de donner au citoyen l'impression qu'un maximum de sécurité est garanti pour protéger les droits fondamentaux de la vie privée des personnes?

Chacun sait que les obligations énumérées à l'article 23 pour assurer la sécurité des traitements ne peuvent être respectées toutes en même temps.

Il est donc illusoire de promettre un maximum de sécurité du traitement des données aux personnes concernées et, par là, le respect des libertés individuelles.

13. *Ad article 26: Le droit à l'information de la personne concernée*

Notre chambre se doit de constater qu'en pratique, ce droit à l'information de la personne concernée est souvent bafoué.

Un article du Monde diplomatique de mai 2000 intitulé „Soupçons sur les banques d'ADN" confirme que, surtout dans le domaine de la génomique, les violations du droit à l'information de la personne concernée sont très fréquentes.

En l'espèce, une fondation pour la recherche se lancait dans la collecte d'ADN de Français âgés de plus de 90 ans, afin de mettre en évidence les mécanismes génétiques de la longévité, c'est-à-dire les gènes dont la présence assurerait une protection naturelle contre les maladies.

A cette fin, la fondation a constitué une banque de données génétiques. A l'insu de l'initiateur et des personnes concernées de ce projet, la direction de la fondation a signé un contrat avec une société de biotechnologie sur la banque de données génétiques dans lequel la fondation touchait, en contrepartie du droit exclusif accordé à cette société à valoriser les résultats de la banque, une contribution financière de 32 millions de FF.

Souvent il arrive que, comme en l'espèce, le responsable du traitement n'est pas le responsable ou représentant de l'entreprise qui, contre le gré du premier, passe outre la procédure d'information.

Vu l'enjeu financier dans les transferts de données génétiques, il n'est pas étonnant que certains avares n'aient pas les moindres scrupules pour se passer du droit à l'information de la personne concernée.

Le plus gênant dans les contrats qui se passent entre laboratoires publics et sociétés privées, c'est qu'ils consentent pour la plupart une exclusivité au payeur sur la banque de données ADN. C'est contre l'intérêt des malades, puisque cela exclut toutes les autres pistes de recherche qui pourraient être menées à partir de cette banque, avec d'autres partenaires.

Voilà pourquoi notre chambre émet ses plus grandes réserves sur l'affirmation que de telles dispositions puissent empêcher des dérives telles que décrites ci-dessus.

14. *Ad article 27: Exceptions au droit à l'information de la personne concernée*

Notre chambre est d'avis que les dérogations à l'article 26 mettent en cause le principe même du droit à l'information de la personne concernée, ceci surtout dans des cas où le justiciable est exposé à des enregistrements d'entretiens téléphoniques, de décryptage des mots de passe etc.

Même dans des domaines comme la sûreté de l'Etat, de la défense, de la sécurité publique et de la recherche d'infractions, notre chambre juge indispensable que la personne suspectée dispose au moins *a posteriori* d'un droit à l'information et au contenu des traitements opérés par les responsables.

Ce droit à l'information est encore plus important si la personne lésée entend attaquer un tel traitement de données en justice. A défaut d'obligation d'informer le justiciable, tout recours contre un tel traitement est voué à l'échec *ab initio*.

Philippe Rivière dans un article du Monde diplomatique, édition mars 1999, confirme les objections formulées par notre chambre en écrivant à ce sujet:

S'il est logique de requérir que „la cible" ne soit pas avertie des modifications (des traitements) effectuées pour exécuter l'ordre d'interception, il est en revanche, plus inquiétant de constater que les opérateurs seront tenus de protéger les informations qu'ils détiennent sur la nature et le nombre des interceptions en cours ou réalisées et de ne pas divulguer les informations liées à la méthode d'interception. Qui, en ce cas, pourrait rendre compte des activités de surveillance?

15. *Ad articles 28 et 29 sur le droit d'accès et ses exceptions*

Mêmes remarques que pour les articles 26 et 27.

L'article 29 ne précise pas dans quels cas le droit d'accès est limité et dans quels autres il est différé. Qu'en est-il par exemple en cas d'écoutes téléphoniques?

La distinction est importante dans la mesure où dans le premier cas il y a une restriction quant à l'accès des données alors que dans le deuxième cas il y a un report dans le temps du droit d'accès.

Comme le responsable doit motiver la limitation ou le report dans le temps du droit d'accès, notre chambre demande qu'il doive motiver sa décision *in concreto* et qu'il ne suffise pas d'indiquer un motif *in abstracto* (p. ex. la recherche d'infractions).

Contrairement au paragraphe (5) in fine, notre chambre est d'avis que la Commission *doit* communiquer à la personne concernée le résultat de ses investigations, *y compris leur contenu*.

16. *Ad article 30: Droit d'opposition de la personne concernée*

Notre chambre se demande comment une personne peut faire opposition contre un traitement dont elle n'a pas connaissance.

Le problème majeur est que, dans la plupart des cas, la personne concernée ignore complètement que des données personnelles la concernant soient traitées.

17. *Ad article 33: Sanctions administratives*

Notre chambre exige que la CNPD n'ait pas seulement pour mission de verrouiller, effacer ou détruire des données, mais également d'enlever ou de démonter les moyens ayant servi au traitement des données.

En effet, notre chambre constate que, dans le cadre de l'article 11 (surveillance sur le lieu de travail), beaucoup de salariés constatent que, malgré une décision de refus rendue suite à une demande d'autorisation préalable de l'employeur auprès de la CNPD, les moyens ayant servi au traitement des données ne sont pas pour autant enlevés de sorte que les salariés ne savent pas si le moyen en cause (p. ex. caméra) est toujours en marche ou non.

18. *Ad article 36: Composition de la Commission Nationale pour la Protection des Données*

En vue de mieux protéger les intérêts des citoyens – en leur qualité de travailleur et de consommateur, notre chambre exige que les organisations syndicales les plus représentatives au niveau national soient également représentées dans la Commission.

19. *Ad article 41: Dispositions spécifiques*

Notre chambre tient à préciser que les articles 88-1 à 88-4 du code d'instruction criminelle ne couvrent pas tous les moyens techniques de surveillance et de contrôle.

Les écoutes téléphoniques étant un de ces moyens, il y a lieu de préciser qu'il existe trois types d'écoute, à savoir les écoutes judiciaires (articles 88-1 et 88-2), les écoutes administratives (articles 88-3 et 88-4) et les écoutes dites sauvages.

Concernant les écoutes judiciaires, notre chambre réfute que cette procédure initialement prévue pour détecter les personnes suspectées de terrorisme et de trafic de drogue soit ouverte à la poursuite de presque toute infraction. Dans les faits, tout juge peut demander à écouter n'importe qui. Il suffit de préciser que c'est pour la bonne cause.

Ceci est d'autant plus contestable que l'écoute judiciaire est absolument indétectable. Impossible donc, pour un particulier de savoir qu'il est écouté.

Les mêmes remarques valent également pour les écoutes administratives qui peuvent être ordonnées par le Premier ministre aux fins de rechercher des infractions contre la sûreté extérieure de l'Etat que un ou plusieurs auteurs tentent de commettre, ou ont commises ou tenté de commettre.

En pratique cependant, il existe un autre moyen de surveillance non prévu par la loi, à savoir les écoutes sauvages. Ces écoutes téléphoniques sont effectuées sans aucun mandat officiel. Contraires aux lois sur le respect de la vie privée, ces écoutes sont souvent utilisées dans des affaires d'espionnage industriel ou, plus prosaïquement, dans des histoires de divorce.

*

III. CONCLUSION

Compte tenu des remarques formulées ci-avant, notre chambre revendique l'instauration de règles coercitives au niveau international afin que la Communauté internationale toute entière soit soumise aux mêmes règles et aux mêmes sanctions. Tant qu'une telle norme de droit international fait défaut, toute législation qui existe à un niveau inférieur est vouée d'office à l'échec, car exposée aux pressions politiques d'autres Etats auxquels une telle législation est inopposable.

Par ailleurs, une telle norme doit être respectueuse des principes de proportionnalité et de finalité et informer le citoyen sur les données qui ont fait l'objet d'un traitement, même et surtout dans le domaine pénal. Ce n'est que si une telle obligation par les autorités publiques d'informer le citoyen existe, que celui-ci dispose d'une voie de recours effective.

Il en résulte que tant le texte de loi actuellement en vigueur que le présent projet de loi ne constituent rien d'autre qu'un coup d'épée dans l'eau plutôt qu'un instrument efficace permettant de garantir un équilibre entre les libertés individuelles, d'une part, et la libre circulation des données à caractère personnel, d'autre part.

Voilà pourquoi notre chambre a le regret de vous informer qu'elle marque son désaccord avec le présent projet de loi, ceci tant quant au fond que quant à la forme.

*

La fraction minoritaire dans la Chambre de travail émet des réserves quant au texte introductif de l'avis 21/2006 intitulé „I. Les libertés individuelles gravement menacées".

La fraction minoritaire se distance formellement du contenu de ce passage de l'avis qui prétend dresser un état des lieux au niveau de la politique mondiale et contient des appréciations tendancieuses, qu'il n'appartient pas, selon la conviction de la fraction minoritaire, à la Chambre de travail d'émettre dans le cadre de ses prérogatives.

L'analyse proprement dite des articles du projet de loi contenue au point II recueille le soutien de la fraction minoritaire.

Luxembourg, le 29 septembre 2006

Pour la Chambre de Travail,

Le Directeur,
Marcel DETAILLE

Le Président,
Henri BOSSI

Service Central des Imprimés de l'Etat