N° 4735[3]

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI

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

* * *

AVIS DE LA CHAMBRE DE TRAVAIL

(14.11.2001)

Par lettre en date du 15 décembre 2000, référence B58071, notre chambre a été saisie pour avis du projet de loi No 4735 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel.

Notre chambre soucieuse de la protection des personnes à l'égard des données à caractère personnel se doit de formuler des remarques tant d'ordre général que ponctuel.

*

I. OBSERVATIONS GENERALES

A. Le projet de loi ne risque-t-il pas d'entraver les droits fondamentaux de la personne?

Le considérant 3 de la directive 95/46/CE dispose que *„l'établissement et le fonctionnement du marché intérieur dans lequel, conformément à l'article 7A du traité, la libre circulation des marchandises, des personnes, des services et des capitaux est assurée, nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un Etat membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés"*.

La directive cherche donc à trouver un équilibre entre la libre circulation des marchandises (données) et la protection des droits fondamentaux de la personne à l'égard de ces données.

Force est cependant de constater que cet „équilibre" se fait au détriment des derniers si l'on se réfère à l'article 1 alinéa 2 de la directive qui dispose que *„les Etats membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre Etats membres pour des raisons relatives à la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée"*.

Cet article n'est que la consécration des articles 28 et 29 du traité de Rome, garants de la libre circulation des marchandises.

Voilà pourquoi le message donné par la Commission européenne est clair: la libre circulation des données prime la protection des personnes à l'égard du traitement des données à caractère personnel.

Le projet de loi a-t-il pour autant repris la philosophie de la directive?

A priori, le lecteur pourrait croire le contraire en lisant l'article 1 qui ne se réfère plus au concept de la libre circulation des marchandises mais uniquement à la protection des droits fondamentaux de la personne.

Les bonnes intentions ne perdurent cependant pas si l'on analyse la suite des articles ainsi que l'exposé des motifs du projet de loi lequel illustre de façon éloquente l'approche de la Commission européenne. Voici quelques passages évocateurs:

„La Commission européenne présenta un paquet de mesures, dont l'objet était d'harmoniser dans les Etats membres de l'Union européenne les législations en matière de protection des données, afin

que celles-ci ne soient plus à l'origine de restrictions ou d'interdictions à la libre circulation des données à caractère personnel dans le marché unique …"

L'harmonisation des législations des Etats membres en matière de protection des données n'est pas une fin en soi, mais un moyen pour promouvoir le marché intérieur.

Voilà pourquoi il est évident que la protection des personnes à l'égard du traitement des données à caractère personnel ne peut être que minimaliste comme le laisse sous-entendre le passage suivant de l'exposé des motifs:

„Le principe de la libre circulation des données est reconnu dans la directive 95/46/CE. Ceci implique nécessairement que l'on passe d'un système d'autorisation préalable à un système de plus grande liberté dans lequel l'autorisation préalable serait réduite à la portion congrue …

La libre circulation des données est un corollaire nécessaire à la liberté du commerce et de l'industrie …

La libre circulation des données est d'autant plus importante que la dimension du Grand-Duché de Luxembourg, sa place financière exigent une facilitation et une accélération des flux de données avec un niveau de sécurité juridique accru."

Notre chambre ne peut, au vu des considérations formulées ci-dessus, partager l'opinion que le projet de loi établit un équilibre entre les intérêts du marché intérieur et la protection des personnes à l'égard des données à caractère personnel.

Elle se permet davantage de démontrer dans l'analyse des articles que les droits fondamentaux de la personne ont été réduits au plus petit dénominateur commun.

B. Légiférer au compte-gouttes accentue davantage l'arbitraire!

Notre chambre conteste catégoriquement la façon de procéder du gouvernement qui consiste à se référer à d'innombrables reprises à des règlements d'application qui pourtant font défaut au moment de la saisine de notre chambre. Ceci va davantage accroître l'arbitraire et l'incohérence en la matière:

– d'abord, dans la mesure où un texte de loi est difficilement applicable si les règlements grand-ducaux auxquels il renvoie n'ont pas encore été élaborés;
– puis, dans la mesure où, à un moment ultérieur, les acteurs de la procédure législative sont obligés de relire le texte de loi ainsi que leurs avis y relatifs pour apprécier la légalité des règlements grand-ducaux.

C. Le projet de loi, un texte indigeste truffé d'exceptions!

Bien que le texte du projet ne fasse plus référence au principe de la libre circulation des marchandises tel qu'évoqué dans la directive, il prévoit dans presque tous les articles tant de dérogations ou de tempéraments à la conception restrictive du traitement des données à caractère personnel que l'on peut avoir l'impression que le principe devient exception et vice versa.

Pour ne citer qu'à titre d'exemple les articles 6 et 7 du projet ayant trait au traitement de catégories particulières de données respectivement au traitement de catégories particulières de données par les services de la santé.

Le paragraphe 1 de l'article 6 établit le principe d'interdiction des données dites sensibles.

Le paragraphe 2 énumère les exceptions qui sont bel et bien au nombre de huit.

L'article 7 continue dans le même flou artistique en prévoyant dans son paragraphe 1 – hormis les exceptions prévues au paragraphe 2 de l'article 6 – une exception supplémentaire au principe d'interdiction de traitement des données dites sensibles de l'article 6 paragraphe 1.

Le paragraphe 2 de l'article 7 prévoit pour le traitement de catégories particulières de données par les services de la santé une autorisation préalable de la Commission.

Le paragraphe 3 du même article prévoit de nouveau des dérogations où pour certains traitements il suffit d'une simple notification.

Le paragraphe 4 de l'article 7 va encore plus loin dans la mesure où un règlement grand-ducal permet de déroger à l'interdiction du traitement de données sensibles lorsqu'il s'agit de les communiquer à des tiers ou de les utiliser à des fins de recherche.

Ici on ouvre encore davantage la brèche aux abus dans la mesure où la loi accorde à un règlement le pouvoir de déroger à ses propres principes et dérogations.

La question épineuse reste de savoir si l'article 7 paragraphe 4 constitue une dérogation aux dérogations des articles 6 et 7 ou bien une dérogation aux principes des articles 6 et 7.

Cette façon de légiférer est inacceptable pour notre chambre. Elle érige en principes les exceptions, et ceci bien évidemment, au détriment de la protection des droits fondamentaux de la personne.

*

II. ANALYSE DES ARTICLES

Deux principes sacro-saints constituent la trame du présent projet, d'une part, le principe de la finalité du traitement des données personnelles et d'autre part, le principe de proportionnalité du traitement des données personnelles.

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

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

C'est au sujet de ces deux principes, qui constituent le fil conducteur du projet, que notre chambre a le plus de réserves à faire.

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

Ad article 5 Légitimité du traitement

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

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

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

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

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

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

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

Ad article 6 Traitement de catégories particulières de données (données sensibles)

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

Tout en étant conscient que le décryptage du génome humain peut être bénéfique pour la société, notre chambre tient néanmoins à remarquer que le traitement ou la transmission de données génétiques

peut aussi être utilisé à d'autres fins, notamment dans le secteur des assurances et des relations de travail entre employeur et salarié afin de n'assurer respectivement n'embaucher que les personnes qui, du point de vue génétique, ne sont pas susceptibles d'être affectées par certaines maladies, plus ou moins graves. Le risque d'une stratification de la société en deux classes, les „génétiquement sains", d'une part et les „génétiquement affectés", d'autre part existe bel et bien.

Qu'arrive-t-il si le salarié ou l'assuré ont donné leur consentement exprès à un tel traitement pour conclure un contrat de travail ou un contrat d'assurance et si la loi n'interdit pas la levée de l'interdiction du traitement des données génétiques?

Le risque est grand que, vu la subordination ou la faiblesse économique du salarié resp. de l'assuré à l'égard de l'employeur resp. de l'assureur qui lui demandent la communication de ses données génétiques, le premier, sous l'effet de l'ignorance et de l'intimidation, donne *nolens volens* son consentement à un tel traitement.

Est-on encore en présence d'un consentement libre et éclairé si la personne en question n'a aucune alternative pour refuser un tel traitement de ses données?

Ad article 10 „Traitement à des fins de surveillance"

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

Notre chambre est d'avis que ce phénomène existe bel et bien déjà et quiconque peut s'apercevoir de l'installation de vidéocaméras installées aux abords des routes ou au centre-ville.

Le paragraphe précité est conçu en des termes si flous et généraux qu'un traitement à des fins de surveillance est possible dans „tout lieu accessible ou non au public (…), pourvu qu'il présente (…) un risque rendant le traitement nécessaire à la prévention, la recherche, la constatation et la poursuite d'infractions pénales".

Ce paragraphe en permettant donc aux autorités d'installer des vidéocaméras un peu partout, comme bon leur semble est contraire au critère de „prévisibilité".

Etant donné que la délinquance au sens large est omniprésente non seulement dans les agglomérations, mais également dans les localités de la campagne (surtout les vols avec effraction), il faudrait donc étendre le dispositif des vidéocaméras à l'entièreté du territoire luxembourgeois si l'on ne veut pas se laisser faire le reproche qu'une infraction commise en province mérite moins d'attention (de surveillance) que dans les centres-villes.

Cette politique a posteriori de surveillance renforcée montre que la mise en oeuvre de l'ouverture des frontières internes de l'Union européenne a entraîné des inconvénients dont on ne pouvait, dès le début, mesurer l'ampleur.

Pour détecter les auteurs d'infractions, les autorités luxembourgeoises sont contraintes de surveiller un peu n'importe qui et n'importe où. Est-il alors exagéré de prétendre que les droits et libertés individuelles des personnes sont réduits à une portion congrue?

Notre chambre a de sérieux doutes que même une prolifération des moyens de surveillance sur tout le territoire – parce que les infractions sont commises un peu partout – réduise de façon considérable le nombre d'infractions. Pour lutter contre la délinquance et la criminalité, l'auteur du projet est prêt à prendre en ôtage (surveiller) la société tout entière. Cette façon de procéder ne peut être acceptée par notre chambre. Elle est plutôt d'avis qu'il faudrait davantage investir dans la formation de la police, dans les réseaux de police interétatiques (Europol) et de doter ceux-ci des moyens en personnel et en matériel nécessaires plutôt que de chercher une solution de facilité – une surveillance renforcée par caméras – qui se fait, d'ores et déjà, au détriment des libertés individuelles des personnes.

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

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

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

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

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

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

Ad article 11 Traitement à des fins de surveillance sur le lieu de travail

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

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

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

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

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

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

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

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

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

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

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

Dans un ordre très subsidiaire, et pour autant qu'un traitement à des fins de surveillance soit indispensable, notre chambre demande que le comité mixte d'entreprise doive pouvoir décider non seulement dans les cas visés aux lettres (a) et (d), mais également dans les cas visés aux lettres (b) et (d),

ceci conformément à la procédure qui est prévue à l'article 16 de la loi du 6 mai 1974 instituant des comités mixtes dans les entreprises. Par ailleurs elle demande d'accorder le même pouvoir de décision aux délégués du personnel, si le comité mixte d'entreprise fait défaut.

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

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

Ad article 14 „Autorisation préalable de la Commission"

Le problème est que, si une telle autorisation n'est pas demandée par le responsable du traitement ou lui est refusée et qu'il utilise ou transmet, malgré tout, des données sensibles à un tiers, les sanctions pénales prévues au paragraphe 3 de cet article ne sauraient tout de même réparer le préjudice subi par la personne qui a fait l'objet du traitement.

Toujours est-il qu'une personne tierce en possession de données personnelles peut, à son tour, de nouveau communiquer celles-ci à une autre personne. Bref, la transmission de données personnelles par le biais de plusieurs responsables de traitement ne peut être effacée *ab initio*.

Concernant le paragraphe 2, notre chambre se demande si l'Inspection du travail et des mines dont l'avis préalable doit être demandé en vue de l'autorisation préalable de la Commission n'a pas un conflit d'intérêts dans la mesure où d'une part, de par la loi du 4 avril 1974 portant réorganisation de l'ITM, elle a pour mission de veiller au respect des conditions de travail des travailleurs, de la sécurité et de la santé au travail et d'autre part, de par la présente loi, elle est obligée de donner son avis sur les conditions de travail (au sens large) dont elle doit elle-même assurer le contrôle.

Ad article 17 „Autorisation par voie réglementaire"

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

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

et

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

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

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

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

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

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

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

Ad article 19 „Dérogations“

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

Il ajoute de l’arbitraire à l’arbitraire.

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

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

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

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

Ad article 21 Confidentialité des traitements

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

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

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

Ad article 22 Sécurité des traitements et ad article 23 Mesures particulières de sécurité

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

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

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

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

Compte tenu de cette réalité, n’est-il pas un peu osé de la part des législateurs européen et national de donner au citoyen l’impression qu’un maximum de sécurité est garanti pour protéger les droits fondamentaux de la vie privée des personnes?

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

Il est donc illusoire de promettre un maximum de sécurité du traitement des données aux personnes concernées.

Ad article 26 Le droit à l’information de la personne concernée

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

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

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

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

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

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

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

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

Ad article 27 Exceptions au droit à l'information de la personne concernée

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

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

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

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

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

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

Mêmes remarques que pour les articles 26 et 27.

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

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

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

Contrairement au paragraphe (4) in fine, notre chambre est d'avis que la Commission *doit* communiquer à la personne concernée le résultat de ses investigations, *y compris leur contenu*.

Ad article 30 Droit d'opposition de la personne concernée

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

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

Ad article 31 Décisions individuelles automatisées

Ce droit de ne pas se soumettre à une décision individuelle automatisée se révèle souvent illusoire.

Y a-t-il des salariés qui oseront s'opposer – même en présence d'un motif raisonnable et légitime – à une telle décision d'un employeur? La conséquence de l'exercice d'un tel droit par le salarié serait probablement qu'il mettrait en péril sa relation de travail.

Ad article 34 Missions et pouvoirs de la Commission Nationale pour la Protection des Données

Notre chambre se demande si, conformément au paragraphe 3(e), la Commission a été préalablement consultée à l'adoption de ce projet de loi et, si dans l'affirmative, pourquoi il n'a pas été annexé au présent projet de loi.

Ad article 36 Composition de la Commission Nationale pour la Protection des Données

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

Ad article 41 Dispositions spécifiques

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

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

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

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

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

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

*

CONCLUSION

Compte tenu des remarques formulées précédemment prouvant à suffisance de droit que les principes de proportionnalité et de finalité de la loi sont voués à l'échec ab initio, notre chambre estime que le projet de loi soulèvera plus de problèmes qu'il n'en résoudra.

Nul n'ignore qu'il peut faire l'objet d'une mesure de surveillance sans qu'il s'en aperçoive, à quelque titre que ce soit. Après les attentats terroristes du 11 septembre 2001 au WTC à New-York et au Pentagone à Washington, cette crainte semble davantage justifiée, comme le témoignent par exemple les projets de mesures que le gouvernement allemand entend mettre en oeuvre sous le prétexte du terrorisme („Rasterfahndung", empreinte digitale de tous les citoyens …).

Rien ne permet de penser que les pratiques de contrôle et de surveillance ayant existé jusqu'à ce jour, en l'absence d'un texte juridique, vont cesser dès l'entrée en vigueur de la présente loi. Certaines pratiques ne sont même pas couvertes par elle comme l'espionnage économique et militaire.

Par ailleurs l'efficacité d'une telle législation est limitée dans la mesure où elle ne couvre que l'espace économique européen, à l'exclusion du reste du monde. Ceci n'empêche donc pas les mesures de surveillance et de contrôle en Europe à partir de pays tiers.

Au lieu de réduire le contentieux en la matière, notre chambre craint que le présent projet de loi n'aggrave l'engorgement des tribunaux. Dans une telle hypothèse, il serait tout à fait incertain et aléatoire comment les tribunaux appliqueraient le principe de proportionnalité en tenant compte des libertés individuelles, d'une part et de l'intérêt collectif, d'autre part.

Finalement notre chambre craint que l'imagination de quelques-uns pour épuiser les lacunes de la loi ne puisse l'emporter sur sa finalité. Si tel était le cas, la loi manquerait son but!

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

Veuillez agréer, Monsieur le Ministre, l'expression de nos sentiments très distingués.

Luxembourg, le 14 novembre 2001.

Le Directeur,
Marcel DETAILLE

Le Président,
Henri BOSSI

Service Central des Imprimés de l'Etat