N° 5554[6]

CHAMBRE DES DEPUTES

Session ordinaire 2006-2007

P R O J E T D E L O I

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 COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES

(5.12.2005)

Par courrier du 21 novembre 2005, Monsieur le Ministre délégué aux Communications a bien voulu soumettre pour avis à la Commission nationale le projet de loi prémentionné, à l'élaboration duquel elle a été associée, en lui demandant de lui faire part d'éventuels commentaires substantiels résiduels.

*

I. CONSIDERATIONS GENERALES

Dans son rapport d'activité pour l'année 2003 et le 1er trimestre 2004 adressé au gouvernement en août 2004, la Commission nationale exprimait son insatisfaction de ne pas être matériellement en mesure de traiter les demandes d'autorisation introduites dans des délais raisonnables et faisait part de sa constatation que l'attention des responsables de fichiers et de traitements de données restait trop focalisée sur l'accomplissement des formalités préalables prévues au chapitre III.

Elle préconisait dès lors une simplification substantielle du régime de déclaration des traitements et un allègement des formalités administratives, allant jusqu'à encourager le gouvernement à envisager de restreindre les traitements de données et cas de figure nécessitant l'autorisation préalable conformément à l'article 14.

Elle souhaitait également voir apporter certaines clarifications dans le texte de la loi ainsi que des modifications susceptibles d'aligner le droit luxembourgeois sur le texte de la directive chaque fois que les écarts n'apparaissaient pas réellement nécessaires ou suffisamment justifiés pour compenser les difficultés d'interprétation et d'application de la loi auxquels ils donnent souvent lieu.

L'intention du gouvernement de procéder rapidement à une révision de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel annoncée solennellement dans le programme de coalition avec comme objectif primaire de clarifier et de simplifier les procédures de façon à éliminer certains obstacles purement administratifs sans plus-value pour la protection de la vie privée et les libertés individuelles, était donc enregistrée avec beaucoup de satisfaction par la Commission nationale pour la protection des données qui annonçait elle-même

vouloir dorénavant mettre davantage l'accent sur ses missions de guidance des responsables de traitements et d'explication de la loi, d'information et, le cas échéant, de contrôle a posteriori plutôt que d'examen des formalités administratives préalables.

Le texte du présent projet de loi procède de cette façon de voir les choses et résout un grand nombre de difficultés actuelles.

Un puissant coup de gouvernail n'était sans doute pas nécessaire, un démantèlement des mécanismes de protection actuels aurait été ressenti comme indéfendable, mais des retouches, clarifications et simplifications susceptibles de faciliter l'application de la loi et de surcroît de désengorger la Commission nationale pour la protection des données étaient hautement souhaitables, y compris certaines modifications au régime applicable aux traitements à des fins de surveillance des articles 10 et 11.

Nous sommes profondément convaincus que la loi doit à la fois être claire et assurer une protection efficace des citoyens. Les formalités administratives n'ont de sens que si elles facilitent l'application des dispositions de la loi.

Celle-ci ne devrait pas être plus ambitieuse que ce qu'on peut raisonnablement espérer voir être appliqué en pratique par les entreprises, les administrations et organisations et autres professionnels normalement diligents.

Des règles de protection qui restent lettres mortes se retournent en pratique contre la crédibilité et l'efficacité du cadre légal et contre celles de l'autorité chargée de veiller à son application.

Pour ces raisons, la Commission nationale pour la protection des données accueille favorablement les modifications proposées dans le projet de loi, y compris certains assouplissements dont elle est convaincue qu'ils sont indispensables pour permettre qu'elle soit mieux respectée et donc renforcer la rigueur de son application.

Dans cet esprit elle a estimé devoir formuler dans les développements qui suivent quelques propositions supplémentaires notamment concernant le régime des traitements à des fins de surveillance dont elle espère qu'elles s'avéreront adoptées aux besoins et possibilités effectives.

Nous nous félicitons donc de l'approche générale de l'avant-projet de loi consistant à apporter les clarifications nécessaires et à simplifier les formalités préalables à la mise en oeuvre des traitements (chapitre III) sans réduire pour autant le niveau général de la protection légale.

Comme Monsieur le Ministre délégué aux Communications l'a fait remarquer lors de la conférence de presse de la Commission nationale pour la protection des données le 25 octobre 2004, la priorité doit revenir à l'établissement et à l'amélioration d'une culture de la protection de la vie privée et des données personnelles au Grand-Duché (l'important est que cela rentre dans les mentalités, pas seulement sur les formulaires).

Ceci concorde avec la vision stratégique de notre Commission nationale qui, à l'instar de ses consoeurs plus prestigieuses dans d'autres Etats membres, entend dorénavant se concentrer de façon privilégiée à l'information du public, l'élaboration d'avis et de recommandations, la guidance des responsables de traitements de données et la promotion des meilleures pratiques en la matière.

*

II. ALLEGEMENT DE LA PROCEDURE DE DECLARATION DES TRAITEMENTS

L'élargissement des exemptions de l'obligation de notification des traitements prévue aux articles 12 et 13 est de nature à répondre non seulement aux souhaits exprimés dans la prise de position du groupe patronal du Comité national pour la simplification administrative en faveur des entreprises, mais suit également les préconisations par le groupe de travail européen des commissaires à la protection des données (Groupe article 29) dans son rapport relatif à la simplification de l'obligation de notification et d'un meilleur usage des exemptions permises par la directive[1].

Le groupe européen des commissaires à la protection des données s'est en effet déclaré favorable à l'introduction d'un éventail plus large d'exemptions dans les législations nationales pour dispenser de la formalité administrative les traitements de données les plus courants qui ne sont normalement pas susceptibles de porter atteinte à la sphère privée des individus.

---

1 WP 106 du 18 janvier 2005; (http://europa.eu.int/comm/justice_home/fsi/privacy/docs/wpdocs/2005/wp106_en.pdf)

Bien que le catalogue des exemptions de l'obligation de notification qu'il est proposé de rajouter à l'article 12 soit bien moins volumineux que les exemples analysés par le groupe patronal du CNSAE dans son papier de réflexion, les cas d'ouverture sont décrits de façon plus large et générale de sorte que dans l'application pratique l'impact de la modification proposée devrait se rapprocher de celui du décret afférent pris au Pays-Bas dont le texte s'étend tout de même sur 76 pages.

Les Pays-Bas ont également repris dans leur législation de façon optionnelle pour les responsables de fichiers et traitements l'institution du détaché à la protection des données comme cas d'exemption de l'obligation de notification. Le rapport du Groupe de l'article 29 relate en outre les expériences positives faites en Allemagne, puis en Suède et aux Pays-Bas avec l'institution du chargé de la protection des données propre à l'établissement (betrieblicher Datenschutzbeauftragter) comme alternative à l'obligation de notification.

Cette exemption qui a également été introduite il y a un an dans la loi française figure déjà dans la loi du 2 août 2002 comme une faculté optionnelle pour les responsables du traitement.

Le chargé de la protection des données

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

Il résulte d'une récente note de synthèse publiée par la CNIL sur les détachés à la protection des données et intitulée „Etude comparée sur les détachés à la protection des données (DPOs) désignés par les responsables de traitement en application de l'article 18 paragraphe 2 de la Directive 95/46/EC[3]" que le premier bilan dans les cinq pays de l'Union européenne ayant opté pour ce régime de simplification est globalement positif. Il s'est en effet avéré que le recours au chargé de la protection dans nos pays voisins a indéniablement contribué à diminuer la bureaucratie, à renforcer une meilleure diffusion de la culture de la protection de la vie privée et à développer l'autorégulation dans divers secteurs d'activité.

A. *L'élargissement du cercle des personnes pouvant être désignées comme chargé de la protection des données*

Jusqu'à présent le chargé de la protection des données ne peut être salarié du responsable du traitement. Cette incompatibilité avait été jugée nécessaire par le législateur en 2002 pour suffire au critère d'indépendance requise par la directive.

L'assouplissement du dispositif, en permettant à l'avenir également à un salarié du responsable du traitement d'assurer la mission du chargé de la protection des données, rendra ce régime encore plus attractif. Il va sans dire que le chargé de la protection des données doit exercer son jugement en dehors de toute pression et présenter ses conclusions sans parti pris, du fait qu'il aura à apprécier la licéité de traitements portant, par exemple, sur la surveillance de l'activité du personnel ou qu'il aura pour devoir de préconiser des solutions organisationnelles ou technologiques qui pourraient ne pas recueillir immédiatement l'assentiment de sa hiérarchie ou des services concernés.

Conformément à l'article 18 de la directive européenne 95/46/CE (repris au paragraphe 3 de l'article 40 de la loi), le détaché doit pouvoir exercer ses fonctions en toute indépendance. Plusieurs éléments ont été identifiés par les Etats membres pour traduire l'exigence d'indépendance posée dans la directive.

- **La liberté d'action du chargé de la protection des données**

  Le positionnement hiérarchique ou encore la possibilité pour le détaché d'en référer directement au responsable de traitement sont retenus comme critères-clés de son indépendance. La loi allemande

---

2 cf. document parlementaire 4735[13], p. 38.

3 http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CIL/dpo-comparaison-UE-VD.pdf

prévoit ainsi que le détaché doit être rattaché directement au directeur de la société ou de l'organisation.

- **L'absence de conflit d'intérêts**

  Il est évident que le détaché ne doit pas voir son jugement altéré en raison d'autres fonctions qu'il exercerait parallèlement. L'indépendance dans l'exercice de ses missions implique également qu'il ne puisse être amené à se contrôler lui-même.

  – En Allemagne

    Cette notion de „conflit d'intérêt" est au cœur du choix du *„Datenschutzbeauftragter"* (ci-après „DSB") en Allemagne, où une incompatibilité stricte en a été déduite avec des fonctions de direction de l'organisme. Des conflits d'intérêt ont également été relevés lorsque le DSB occupe également des fonctions dans les domaines ayant trait à la gestion des ressources humaines, à l'administration des systèmes d'information, aux technologies de l'information, ainsi que tout département mettant en oeuvre des traitements de données sensibles ou de grande envergure (par exemple: marketing).

    L'absence de conflit d'intérêt s'apprécie au cas par cas et, en Allemagne, les autorités de contrôle compétentes, saisies le plus souvent par des salariés, interviennent régulièrement pour obtenir, à l'amiable ou sous la contrainte, la décharge du DSB ne remplissant pas ou plus cette exigence.

  – En France

    La notion de conflit d'intérêts a aussi été reprise dans la réglementation française, „les fonctions ou activités exercées concurremment par le correspondant ne doivent pas être susceptibles de provoquer un conflit d'intérêts avec l'exercice de sa mission".[4]

    L'indépendance du correspondant français est renforcée par le fait qu'il „ne reçoit aucune instruction pour l'exercice de sa mission". La législation française prévoit un devoir de collaboration active à charge du responsable du traitement, que le correspondant soit salarié ou non. Le texte allemand va dans le même sens.[5]

Il est à relever que le système français du correspondant à la protection des données à caractère personnel, introduit par un décret No 2005-1309 du 20 octobre 2005, prévoit un régime qui rappelle le statut du travailleur désigné, tout en rajoutant quelques dispositions supplémentaires intéressantes:

– obligation de porter la désignation d'un correspondant à la connaissance des représentants du personnel;
– le correspondant exerce sa mission directement auprès du responsable du traitement et ne dispose donc pas d'autre supérieur hiérarchique;
– le correspondant ne reçoit aucune instruction dans l'exercice de sa mission;
– la fonction de correspondant et de responsable de traitement ou son représentant légal ne peuvent être cumulées;
– les fonctions ou activités exercées concurremment par le correspondant ne doivent pas être susceptibles de provoquer un conflit d'intérêts;
– le responsable du traitement doit collaborer activement à la mission du correspondant;
– le correspondant doit établir un bilan annuel qui doit être présenté au responsable de traitement et à la Commission.

La loi allemande rajoute encore quelques éléments intéressants, qui ne se retrouvent pas dans le texte français:

---

4 cf. article 46 du décret No 2005-1309 du 20 octobre 2005 (JO No 247 du 22 octobre 2005); http://www.cnil.fr/index.pho?id=1880

*„**Art. 46.** Le correspondant à la protection des données à caractère personnel exerce sa mission directement auprès du responsable des traitements.*

Le correspondant ne reçoit aucune instruction pour l'exercice de sa mission.

Le responsable des traitements ou son représentant légal ne peut être désigné comme correspondant.

Les fonctions ou activités exercées concurremment par le correspondant ne doivent pas être susceptibles de provoquer un conflit d'intérêts avec l'exercice de sa mission."

5 *„Die öffentlichen und nicht-öffentlichen Stellen haben den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hlifspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen."*

– ne peut être désignée DSB qu'une personne particulièrement qualifiée;
– le DSB ne doit pas subir de préjudice ou de désavantage en raison de l'exercice de ses fonctions;
– obligation à charge du responsable du traitement de collaborer avec le DSB et de lui fournir tous les moyens nécessaires à l'exercice de ses fonctions (locaux, effectifs, etc.).

Les idées les plus importantes ont été reprises dans le projet de loi par l'ajout de 2 alinéas à l'article 40 paragraphe (3) et l'insertion d'un paragraphe (4).

Il nous paraît toutefois indiqué de proposer au gouvernement d'envisager quelques modifications complémentaires pour parfaire le régime juridique s'appliquant au chargé de la protection des données:

– *il peut être utile d'ajouter que le chargé n'agit pas sur instruction du responsable, mais gère indépendamment sa mission.*

  Cette précision aurait le mérite d'être plus claire et directe que le seul fait d'affirmer l'indépendance du chargé.

– *le responsable du traitement doit collaborer avec le chargé et doit mettre à sa disposition tous les moyens nécessaires à l'exécution de sa mission.*

  L'absence d'une telle disposition risquerait d'encourager des entreprises d'entraver l'exercice de la mission en gardant une attitude complètement passive.

– *finalement, on peut également s'interroger sur l'opportunité de créer une sanction spécifique à l'encontre de l'employeur en cas de violation de ces dispositions.*

*

III. LE REGIME DE L'AUTORISATION PREALABLE

Quant au régime de l'examen préalable (correspondant à l'article 20 de la directive), un resserrement du nombre des traitements de données qui doivent faire l'objet d'une autorisation, conformément à l'article 14 de la loi, avant leur mise en oeuvre se justifie non seulement pour des raisons pratiques (en vue d'aboutir à un désengorgement de la Commission nationale pour la protection des données) mais est également conforme à l'esprit de la directive et à la tendance générale observée ces dernières années dans les autres Etats membres.

Au voeu du considérant 54, le nombre de ceux (traitements de données) présentant des risques particuliers (au regard des droits et des libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités ou du fait de l'usage particulier d'une technologie nouvelle) devrait être très restreint.

Ainsi la loi française, à l'instar de celles d'autres pays, ne soumet également à l'examen préalable de la CNIL le traitement de données sensibles que dans certains cas de figure.

En revanche elle prévoit ce régime renforcé notamment pour (Article 25 de la loi française):

1) certains traitements de données sensibles
2) les traitements portant sur des données génétiques
3) ceux portant sur les infractions et condamnations pénales, sauf s'ils sont mis en oeuvre par les auxiliaires de justice dans le cadre de leurs missions
4) les traitements susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire (effet discriminatoire)
5) l'interconnexion de fichiers dont les finalités sont différentes
6) les traitements portant sur des données parmi lesquelles figurent le numéro d'inscription des personnes ou répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire
7) les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes
8) ceux comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

L'avant-projet de loi s'inspire de ce catalogue de la loi française à l'exception des points 3), 6) et 7).

Au sujet du point 6) ci-dessus, la Commission nationale profite de l'occasion pour rappeler au gouvernement la nécessité de procéder à une révision de la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales et le répertoire afférent et se réfère à ce sujet à ses observations exprimées dans le cadre de son avis relatif au projet de règlement grand-ducal pris en exécution de la loi du 11 novembre 2003 relative à la publicité foncière[6].

L'évolution récente fait apparaître que les conditions prévues par la loi du 30 mars 1979 ne sont plus respectées dans bien des cas et que ce texte ne répond plus à l'exigence de l'article 8 paragraphe 7 de la directive 95/46/CE du 24 octobre 1995 sur la protection des données personnelles qui dispose que les Etats membres déterminent les conditions dans lesquelles un numéro national d'identification peut faire l'objet d'un traitement.

Pour le surplus, les modifications et clarifications proposées dans l'avant-projet de loi concernant les données sensibles (articles 6 et 7), les traitements réalisés dans le cadre de la liberté d'expression (article 9), à la surveillance (articles 10 et 11), à l'interconnexion de données (article 16), les traitements relatifs au crédit et à la solvabilité des personnes (article 14) et au régime de l'autorisation préalable lui-même recueillent l'adhésion des membres de la Commission nationale.

Nous considérons toutefois que quelques assouplissements supplémentaires se justifieraient dans un souci de réalisme et d'adaptation du cadre légal à ce qui pourra être appliqué rigoureusement au jour le jour, et donc en fin de compte, de crédibilité de la loi.

A. Le régime des traitements à des fins de surveillance

Il résulte des travaux parlementaires que le législateur entendait mettre en place un cadre légal assez restrictif pour la mise en oeuvre des traitements de données à des fins de surveillance et cela aussi bien pour ceux opérés par l'employeur à l'égard de ses salariés sur le lieu de travail (article 11) et que pour ceux exercés par tout autre responsable du traitement envers des tiers (article 10).

Cette volonté d'instituer une protection efficace[7] s'est accompagnée du souci que les dispositions adoptées soient claires et assurent dans l'intérêt de toutes les parties en cause la sécurité juridique nécessaire puisqu'elles sont assorties de sanctions pénales. Elle s'est traduite pour ces types de traitements par une dérogation à l'article 5 qui définit les causes légitimes d'un traitement de données à caractère personnel en reprenant celles de l'article 7 de la directive.

Conformément au considérant 30 de la directive les Etats membres peuvent préciser dans leur loi nationale quand l'intérêt légitime du responsable du traitement ou bien les libertés et droits fondamentaux de la personne concernée prévaut en particulier dans le cadre des activités légitimes de gestion des entreprises et autres organisations.

La dérogation retenue consistait à insérer dans le texte des articles 10 et 11 une énumération limitative des conditions de légitimité qui doivent être réunies pour rendre la surveillance et le traitement des données afférentes licites, les cas d'ouverture étant décrits de façon plus précise que dans les critères de légitimation généraux de la directive auquel il n'est dérogé cependant que dans le but de la clarification et de la sécurité juridique (sinon il y aurait transposition incorrecte de la directive).

Par ailleurs, le consentement des personnes concernées est exclu comme critère de légitimation d'une surveillance des salariés sur leur lieu de travail mis en oeuvre par l'employeur.

Cette approche très rigoureuse répond à la grande sensibilité du public à l'égard du recours à des moyens techniques pour contrôler les allers et venues et les comportements des citoyens, en particulier s'ils sont mis en oeuvre dans les lieux publics, accessibles au public et sur le lieu de travail.

Le régime légal des traitements à des fins de surveillance continue à donner lieu à certaines critiques alors qu'une autorisation préalable est requise dans tous les cas énumérés tant à l'article 10 qu'à l'article 11 et que ces catalogues ne prévoient parfois pas de cas d'ouverture permettant d'autoriser des mesures de surveillance dans des circonstances ou pour un but déterminé que l'entreprise, l'administration ou l'organisation considère toutefois comme suffisamment graves pour les légitimer.

---

6 Avis de la Commission nationale pour la protection des données au sujet de l'avant-projet de règlement grand-ducal concernant l'accès au répertoire général des personnes physiques et morales par les officiers publics et autres créateurs ou exécuteurs d'actes translatifs de propriété immobilière ou de constitution d'hypothèque, délibération No 2/2004 du 9 janvier 2004

7 (Doc. parlem. 4735[13] page 19)

Les organisations représentatives des employeurs[8] ont tendance à qualifier les choix opérés par le législateur dans le libellé des articles 10 et 11 comme trop restrictifs et comme ne tenant pas assez compte de l'évolution des techniques et pratiques professionnelles et notamment de la nécessité pour l'employeur qui assure la responsabilité économique de l'exploitation de l'entreprise et de sa pérennité (y compris les incidences sociales) et auquel revient dès lors le pouvoir de direction dans celle-ci, d'avoir les moyens de combattre la fraude, l'usage illégitime des équipements informatiques et d'Internet, de détecter les actes contraires à la loi ou aux bonnes moeurs qui sont susceptibles d'engager la responsabilité de l'employeur ou de lui causer un préjudice économique ou financier.

L'option retenue par le législateur (catalogue détaillé énumérant exhaustivement les cas d'ouverture qui seuls sont reconnus comme légitimes) qui privilégie la protection des personnes et la clarté et prévisibilité de la règle juridique comporte par nature le risque de lacunes dans cette liste limitative et de rigidité de son application.

La Commission nationale pour la protection des données a certes la latitude de nuancer son appréciation de la nécessité et de la proportionnalité des mesures de surveillance envisagées au regard de la finalité poursuivie en fonction du cas de figure précis, des circonstances, du contexte et de suivre dans sa politique l'évolution des pratiques et des moeurs.

Au niveau de la vérification de la légitimité elle ne peut toutefois pallier à l'absence de critère de légitimation et doit toujours se référer à une condition de légitimité expressément prévue dans le texte des articles 10 et 11 pour justifier la délivrance d'une autorisation.

Les trois premières années d'expérience d'examen des dossiers ont permis à la Commission nationale de mettre en évidence une lacune dans les conditions de légitimité de l'article 10 qui s'est traduite par de nombreux cas d'impossibilité de délivrer une autorisation (pour la mise en place d'une vidéosurveillance), notamment pour combattre le vol à l'étalage ou le vandalisme alors que la protection des biens (pourtant prévue à l'article 11) y fait défaut[9].

Par ailleurs, le cas de figure prévu à l'article 11 paragraphe (1) lettre (d) donne lieu à des difficultés d'interprétation et d'application.

Nous notons en outre que la condition de légitimité supplémentaire qu'il était prévu dans la version initiale du projet de loi No 5181 (devenue la loi du 30 mai 2005 relative aux dispositions spécifiques de protection des personnes à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques) de rajouter à l'article 11 de la loi du 2 août 2002 „pour assurer la prévention, la recherche et la détection d'actes susceptibles d'engager la responsabilité de l'employeur" ne se retrouve pas dans l'avant-projet de loi[10].

Tenant compte de tous ces éléments et de l'expérience acquise à ce jour par notre Commission nationale, qui n'arrive malheureusement pas à évacuer dans des délais raisonnables les nombreux dossiers de demandes d'autorisation dont elle est saisie, nous considérons qu'il est possible et souhaitable de voir étendre au régime des articles 10 et 11 de la loi visant les traitements à des fins de surveillance certes de façon mesurée et circonspecte l'effort d'assouplissement et de simplification des formalités administratives à charge des responsables de traitement sans affecter sensiblement le niveau de protection assuré par la loi.

Il apparaît qu'au niveau européen une grande majorité des pays ne disposent pas de cadre légal à portée générale en matière de surveillance sur le lieu du travail. Certes, il est communément admis que la législation relative à la protection des données y trouve application[11], ce qui donne cependant fréquemment lieu à des difficultés d'interprétation. Certaines législations européennes règlent des aspects spécifiques comme par exemple le contrôle par l'employeur de l'usage des courriers électroniques et de la navigation sur Internet ou le recours à la vidéosurveillance.

---

8 cf. papier de réflexion du groupe patronal au sein du CNSAE du 12 juillet 2005 relatif à la réforme et simplification de certaines dispositions de la loi du 2 août 2002 sur la protection des données

9 cf. Cyril Pierre-Beausse. La Protection des données personnelles (éditions Promoculture 2004) No 171: „Un cas d'ouverture manquant: La surveillance des biens".

10 Voir aussi Cyril Pierre-Beausse: ouvrage prémentionné No 190: „Un cas d'ouverture manquant: la mise en cause de la responsabilité du responsable du traitement".

11 Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel adopté le 13 septembre 2001 par le Groupe de travail „Article 29"; doc. WP48; http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2001/wp48fr.pdf

Enfin, la plupart des pays européens reconnaissent aux organes représentatifs certains droits ou pouvoirs en rapport avec la mise en place et/ou l'utilisation de système de surveillance par l'employeur[12].

En ce qui concerne la vidéosurveillance, seuls deux pays européens prévoient dans leur législation-cadre relative à la protection des données un examen préalable à la mise en oeuvre d'un système de surveillance par caméras, à savoir le Portugal, sous certaines conditions, et le Luxembourg. Dans un certain nombre d'Etats membres[13] (l'Allemagne, le Danemark, l'Espagne, la France, les Pays-Bas, le Portugal, la Suède et l'Autriche) des législations spécifiques ont été prises pour réglementer la vidéo-surveillance, mais elles ont la plupart du temps un champ d'application limité (p.ex. limité aux lieux publics ou ouverts au public). Parmi elles, certaines requièrent des autorisations administratives (p.ex. vidéosurveillance des espaces publics en France ou en Suède).

Il convient de se rendre compte que la loi luxembourgeoise assure une protection triplement renforcée des personnes à l'égard de traitements de données à des fins de surveillance par rapport au régime de la directive 95/46/CE du 24 octobre 1995 qu'elle transpose par les spécificités suivantes:

- catalogue restreint et détaillé des conditions de légitimité éligibles
- examen préalable par la Commission nationale pour la protection des données dont l'autorisation requise tient compte également de la balance des intérêts en cause (nécessité et proportionnalité des mesures de surveillance envisagées)
- exclusion du consentement des salariés comme critère de légitimation d'une surveillance mise en oeuvre par l'employeur sur le lieu de travail.

Sur 1.100 demandes introduites entre le ler janvier 2003 et 31 juin 2005 plus de 800 (72%) portent sur des traitements à des fins de surveillance dont une très forte proportion est destinée à s'exercer au moins partiellement à l'égard des salariés (dans des proportions à peu près équivalentes sous forme de vidéosurveillance (182), surveillance de l'usage de la messagerie électronique, de l'ordinateur et d'Internet (139), surveillance des horaires de travail (131), contrôle d'accès des bàtiments (122) et surveillance des conversations téléphoniques (y compris enregistrement) (120)).

B. Modifications proposées

Article 10: Traitements à des fins de surveillance

1ère Proposition: 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 …"*

Commentaire:

Il s'agit de rajouter une condition de légitimité supplémentaire pour la mise en oeuvre de traitements à des fins de surveillance (la plupart du temps par caméras vidéo) visant à endiguer des actes de vandalisme ou de vol.

Il apparaît incohérent que la protection des biens de l'entreprise figure parmi les critères de légitimation d'une surveillance mise en oeuvre par l'employeur à l'égard de ses salariés sur le lieu de travail (article 11 paragraphe 1 lettre (b)) alors que l'autorisation afférente ne peut pas être accordée pour la surveillance de tiers, si ce n'est en cas de nécessité pour la sécurité (physique) des usagers ou la prévention d'accidents.

S'il ne s'agit pas en l'espèce d'un simple oubli du législateur, le texte actuel de la loi est en décalage manifeste avec des pratiques largement répandues – y compris dans notre pays – et acceptées par le public découlant de la constatation, que dans certains cas une surveillance (notamment par caméras vidéo) peut être nécessaire même en l'absence de risques pour l'intégrité physique des personnes, mais pour prévenir et réduire des actes de vandalisme et des vols fréquents et importants. Encore faut-il que la prolifération de ces dispositifs soient juridiquement encadrée et limitée.

---

12 cf. tableau comparatif, annexe 1

13 cf. résumé synthétique, annexe 2

Il y a lieu de noter que la rédaction proposée requiert la justification d'un risque caractérisé et que le pouvoir d'appréciation laissé à la Commission nationale pour la protection des données lui permettra donc d'écarter les dossiers dans lesquels les circonstances ne font pas apparaître une nécessité effective et importante ou laissent subsister des doutes quant au caractère excessif (principe de proportionnalité) du traitement envisagé.

2ème Proposition: Limiter les traitements à des fins de surveillance énumérés à l'article 14 paragraphe (2) comme soumis à l'autorisation préalable de la Commission nationale à ceux prévus à l'alinéa (b) du paragraphe 1er de l'article 10.

Commentaire:

La modification proposée tend à restreindre les traitements à des fins de surveillance prévus à l'article 10 soumis à l'examen préalable de la Commission nationale pour la protection des données à ceux visés à la lettre (b).

Il nous paraît en effet défendable de se contenter de la formalité de la notification préalable à la mise en oeuvre pour les mesures de surveillance pour lesquelles le responsable du traitement a obtenu le consentement des personnes concernées (article 10 paragraphe 1er lettre (a)) et pour celles qu'il entend exercer pour sécuriser les lieux d'accès privé où il est domicilié (ou établi). Les règles de fond applicables resteraient inchangées.

Le critère de légitimation continuera à être requis.

Les doutes quant à la licéité du traitement (apparus à l'examen des notifications) et les abus éventuels relevés par les personnes concernées pourront déclencher des investigations dans le cadre du contrôle a posteriori exercé par la Commission nationale pour la protection des données de sa propre initiative ou sur plainte d'une personne concernée et déboucher le cas échéant sur des sanctions.

L'obligation du responsable du traitement d'informer les personnes concernées au sujet de la surveillance opérée conformément aux articles 10 paragraphe 2 et 26 la transparence, reste elle aussi obligatoire et assortie de sanctions pénales.

Par contre le nombre de dossiers de demandes d'autorisation de traitements à des fins de surveillance devrait diminuer sensiblement et de ce fait réduire les délais de traitement des formalités administratives qui encombrent actuellement la Commission nationale.

Signalons que dans le cadre des travaux préparatoires[14] de la réforme de la loi française (loi du 4 août 2004) sur l'Informatique et les Libertés, un amendement visant à soumettre à l'autorisation préalable de la CNIL „tout traitement relatif à la vidéosurveillance" a été rejeté et que les rapporteurs du Sénat (M. Alex Turk) et de l'Assemblée nationale (M. Francis Delattre), respectivement Président et membre de la CNIL, ont émis tous les deux un avis défavorable au motif qu'il ne serait „pas nécessaire ni pensable de soumettre au système d'autorisation préalable toutes les vidéosurveillances qui se mettent actuellement en place dans le pays".

La vidéosurveillance des espaces publics en revanche y fait l'objet d'une loi spéciale et requiert l'autorisation du préfet prise après avis d'une commission départementale présidée par un magistrat de l'ordre judiciaire.

A notre avis les cas de figure visés à l'alinéa (b) du paragraphe 1er de l'article 10 sont ceux où l'appréciation de la balance des intérêts en cause et des critères de nécessité et de proportionnalité est la plus délicate à opérer et justifie dès lors pour des motifs de sécurité juridique et de protection des personnes, l'exigence d'une autorisation préalable.

---

14 http://ameli.senat.fr/amendements/2001-2002/203/Amdt_101.html (amendement de Monsieur Bret/1ère lecture)
http://ameli.senat.fr/amendements/2003-2004/285/Amdt_8.html (amendement de Monsieur Bret/2ème lecture)
http://www.senat.fr/seances/s200407/s20040715/s20040715002.html#Int1177 (compte rendu intégral des débats au sénat 2ème lecture/15 juillet 2004)
http://www.assembleenationale.fr/12/cri/2003-2004/20040205.asp#P158_8086 (compte rendu intégral des débats à l'assemblée 2ème lecture/29 avril 2004)
http://www.assembleenationale.fr/12/pdf/cri/2003-2004/cahiers/c20040205.pdf (amendements pour la séance du 29 avril 2004)

Article 11: Traitements à des fins de surveillance sur le lieu de travail

Proposition: diviser l'alinéa (d) du 1er paragraphe de l'article 11 en deux points distincts et rajouter une référence à la lettre (f) dans le 2ème alinéa du 1er paragraphe du même article visant les pouvoirs du Comité mixte:

„d) pour le contrôle de la production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte. La surveillance peut seulement être exercée de façon permanente si l'ingérence dans la vie privée des travailleurs est réduite au minimum.

f) pour le contrôle temporaire de l'activité et des prestations du travailleur lorsqu'une telle mesure est nécessaire:

- *pour assurer la prévention, la recherche et la détection d'actes illicites ou susceptibles d'engager la responsabilité de l'employeur, ou*
- *pour la protection des intérêts économiques, commerciaux ou financiers de l'employeur, ou*
- *pour des besoins de formation des travailleurs ou pour l'évaluation et l'amélioration de l'organisation du travail, ou …"*

Commentaire:

• Ad lettre (d):

Le cas de figure visé par le texte actuel de l'article 11 paragraphe 1er lettre (d) nécessite presque toujours que le moyen technique de contrôle soit actif en permanence, sinon comment assurer que les éléments recensés soient exacts et complets pour calculer la rémunération.

La Commission nationale ne peut donc pas se baser sur ce cas d'ouverture pour autoriser un traitement à des fins de surveillance visant à opérer un contrôle continu et permanent des prestations des travailleurs (aucune autorisation n'a encore été accordée sur son fondement). Le critère de légitimation prévu par le législateur s'avère en fin de compte inopérant en pratique. Pour cette raison nous estimons nécessaire de supprimer l'exigence que le contrôle ne s'exerce que de façon temporaire sur les travailleurs.

Certes, l'idée qu'une surveillance, visant à. évaluer le comportement et les performances du salarié, ne doit jamais être que ponctuelle ou temporaire reflète la politique des autorités nationales de surveillance compétentes dans les autres pays en matière de protection des données.[15]

Pour cette raison, il est proposé d'ajouter une condition supplémentaire *(l'ingérence dans la vie privée des travailleurs devra être réduite au minimum)* pour restreindre le nombre de cas où les travailleurs pourront être exposés à une surveillance en continu.

Prenons pour exemple un travailleur spécialisé d'une usine de faïencerie dont la fonction consiste à apposer la décoration sur les pièces de vaisselle en porcelaine en fabrication et qui est payée à la pièce. Assurément un contrôle ponctuel ne permettra pas de déterminer sa rémunération exacte, l'identification et le comptage des pièces fabriquées n'étant pas assurés de façon complète et fiable.

Un mécanisme technique intégré à la chaîne de fabrication qui détermine de façon automatique le nombre de tasses (assiettes, sous-coupes, …) décorées peut s'avérer adapté aux besoins (un cliquet assurant le comptage des pièces) de la détermination automatique des éléments de la rémunération tout en n'affectant que faiblement la sphère privée de la travailleuse.

Par contre une surveillance par caméra vidéo ne devrait pas être autorisée dans le même but, du moins si le travailleur se trouve en plein champ de vision, car il est généralement admis que les travailleurs ne peuvent être – sauf cas exceptionnels (caissiers d'une banque) – exposés à travailler en permanence sous le contrôle de caméras.

---

15 – Avis 8/2001 (WP 48) du 13 septembre 2001 du Groupe de l'Article 29 sur les traitements de données à caractère personnel dans le contexte professionnel (http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2001/wp48fr.pdf);

– La cybersurveillance des salariés (http://lesrapports.la documentationfrancaise.fr/BRP/044000175/0000.pdf);

– Document guide de l'autorité suisse relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail (http://www.edsb.ch/f/doku/leitfaeden/internet/index.htm).

Rappelons ici à toutes fins utiles qu'une jurisprudence constante admet depuis quelques années que le salarié a le droit au respect de sa vie privée, y compris sur son lieu de travail pendant le temps de travail[16], et qu'il est parfois difficile de démêler dans son activité et son comportement sur le lieu de travail ce qui relève de la vie privée et de sa fonction professionnelle.

L'employeur ne peut donc exiger le droit de contrôler (notamment par les moyens techniques modernes) dans le détail et à tout instant, l'ensemble de l'activité de ses salariés.

Par ailleurs, le droit à la protection de la vie privée et des données personnelles lui commande de privilégier les moyens de surveillance les moins intrusifs.

La Commission nationale examine cet aspect dans chaque dossier de demande d'autorisation et s'est vu amener souvent à soumettre le traitement à des conditions spécifiques.

Le fait de préciser dans ce cas d'ouverture de l'article 11 (le seul qui pourrait donner lieu à une surveillance continue et permanente) que *l'ingérence dans la vie privée des travailleurs doit être réduite à un minimum* ne constitue donc qu'un rappel du principe de proportionnalité qui doit être appliqué au contenu des données et aux opérations de traitement des données personnelles envisagés.

• Ad Nouvelle lettre (f):

Concernant l'article 11, les travaux parlementaires de la loi du 2 août 2002 s'étaient basés principalement sur la convention collective de travail No 68 relative à la surveillance par caméras sur le lieu de travail[17] applicable en Belgique.

Le législateur avait voulu arbitrer en faveur d'une forte protection des travailleurs et d'une sécurité juridique dont bénéficieraient en fin de compte toutes les parties en cause, en soumettant tous les traitements par l'employeur à l'égard de ses salariés à l'examen préalable de la Commission nationale et en adoptant un catalogue précis et limitatif de conditions de légitimité.

Nous pensons que cette démarche très protectrice doit être maintenue pour que la surveillance automatisée/électronique ne devienne pas omniprésente sur les lieux de travail, l'employeur gardant par ailleurs toutes les prérogatives découlant de son pouvoir de direction de l'entreprise (ou de l'organisation) qui est la contrepartie de sa responsabilité économique et sociale, mais il devra l'exercer généralement par les moyens traditionnels de la gestion de ses ressources humaines et de son organisation.

En revanche les arguments que le groupe patronal a fait valoir dans le cadre du CNSAE se recouvrent partiellement avec des difficultés et hésitations éprouvées également par la Commission nationale pour la protection des données dans l'application de la loi au cours de sa jeune expérience de l'examen de ces dossiers (les plus nombreux parmi les demandes d'autorisation).

Nous estimons en effet qu'il subsiste des circonstances non couvertes par le catalogue restrictif des cas d'ouverture énumérés à l'article 11 et qu'il est possible de le compléter sans dénaturer l'esprit de la loi en s'inspirant de ladite convention collective belge et de celle No 81 relative au contrôle des communications électroniques en réseau[18] adoptée le 26 avril 2002 et également d'application généralisée en Belgique.

La formulation du *nouvel alinéa (f)* proposé se limite donc à reprendre certains cas d'ouverture figurant dans ces textes belges qui aux yeux de la Commission nationale peuvent justifier dans certains cas la mise en place de dispositif de surveillance. Il reste pourtant très limitatif, afin de ne pas trahir l'esprit du législateur de 2002. Il y a lieu de garder à l'esprit que la Commission nationale pour la protection des données ne peut accorder d'autorisation que dans les cas où la loi prévoit une condition de légitimité.

Quand tel est le cas, elle a en outre l'obligation de scruter consciencieusement la demande pour se rendre compte si les critères de nécessité et de proportionnalité sont bien remplis.

---

16 Cour européenne des Droits de l'Homme: affaire Niemietz c/ Allemagne, 16 décembre 1992
Cour de cassation française, Chambre sociale: – Arrêt Nikon du 2 octobre 2001 et
– Arrêt NAMS du 10 novembre 2005

17 et http://www.cnt-nar.be/CCT/cot-68.doc

18 http://www.cnt-nar.be/CCT/cct-81.doc

Compléter le texte de l'article 11 par l'ajout d'un certain nombre de conditions de légitimité supplémentaire ne reviendra donc pas à déclencher une avalanche de nouveaux traitements à des fins de surveillance sur le lieu de travail.

– *pour assurer la prévention,* la recherche et la détection *d'actes illicites* ou susceptibles d'engager *la responsabilité* de l'employeur

  Une telle condition de légitimité correspond au souci de nombreux employeurs de s'assurer que l'utilisation sur le lieu du travail d'Internet par son personnel ne dépasse pas certaines limites généralement fixées dans le règlement intérieur d'entreprise ou dans une „charte informatique" spécifique.

– *pour la protection des intérêts économiques, commerciaux ou financiers de l'employeur*

  Ce critère de légitimation a été inclus dans la convention collective belge pour justifier notamment une surveillance reconnue nécessaire pour éviter la divulgation déloyale de secrets d'affaires ou d'autres renseignements internes confidentiels.

– *pour des besoins de formation des travailleurs ou l'évaluation et l'amélioration de l'organisation du travail*

  Plusieurs demandes d'autorisation de traitements envisagés avec ces finalités ont dû être refusées par le passé à défaut de cas d'ouverture prévu par le législateur. Notons cependant qu'une autorisation n'est concevable pour ce type de traitements (p.ex. ciblé sur le respect des mesures de sécurité au travail) qu'à des conditions très restrictives, en particulier s'ils sont limités dans un laps de temps extrêmement court et que les personnes concernées aient été informées au préalable de façon exhaustive.

La Commission ne manquera sans doute pas de poursuivre sa politique très réservée et prudente en matière de délivrance d'autorisations afférentes aux employeurs. Rappelons finalement que la loi pose en outre l'accord du Comité mixte comme préalable à la décision de mise en oeuvre d'un tel traitement de données à des fins de surveillance sur le lieu de travail (dans les entreprises ou établissements où un tel organe existe).

Article 14: Autorisation préalable de la Commission nationale

Proposition: remplacer à l'article 14 paragraphe (1) la teneur de la lettre (b) par le texte suivant:

„les traitements à des fins de surveillance visés:

– *à l'article 10 paragraphe (1) lettre (b) dès lors que les données résultant de la surveillance font l'objet d'un enregistrement et à l'article 11 de la présente loi."*

Commentaire:

Cette proposition est déjà commentée sous l'article 10 à la page 12.

*

IV. AUTRES MODIFICATIONS

Article 6 paragraphe 2 lettre (a) et paragraphe 3 lettre (d) (Qualification du consentement)

L'article 8 paragraphe 2 lettre (a) de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à. caractère personnel définit le consentement de la personne concernée de façon plus restrictive lorsqu'il doit légitimer une exception au principe d'interdiction du traitement des données dites „sensibles". Le consentement implicite est exclu du fait que la directive rajoute l'adjectif „explicite" au terme consentement. Nous proposons d'aligner la teneur de la loi au libellé de la directive.

Proposition: insérer à l'article 6 paragraphe (2) lettre (a) ainsi qu'au paragraphe (3) lettre (d) premier alinéa du même article chaque fois après le mot „consentement", le terme „explicite"

Commentaire:

Compte tenu des modifications apportées à la définition du „consentement" à l'article 2 lettre (c), il est indiqué d'ajouter le terme „explicite" aux endroits indiqués à l'article 6, afin que la loi soit pleinement conforme aux exigences de l'article 8 de la Directive 95/46/CE.

Dans le domaine des traitements de données par les services de santé il appartiendra au règlement grand-ducal prévu au paragraphe (4) de l'article 7 de préciser dans quelles circonstances le consentement est requis comme garantie appropriée supplémentaire et s'il doit à son tour être explicite.

En effet les cas de figure visés (médecine préventive, diagnostics médicaux, administration de soins et traitements, recherche scientifique, gestion des services de santé) sont basés sur des finalités limitativement énumérées et des conditions de légitimité propres indépendantes du consentement de la personne concernée (sauvegarde de l'intérêt vital, obligation légale, mission d'intérêt public respectivement nécessité découlant de l'exécution d'un contrat auquel la personne concernée est partie).

Articles 26 à 31: Droits de la personne concernée

La Commission nationale pour la protection des données se félicite des modifications opérées au niveau des droits de la personne concernée visés par les articles 26 et 31 de la loi qui consistent à améliorer la clarté des dispositions afférentes respectivement dans leur alignement sur le texte de la directive. Elle estime cependant nécessaire de réitérer ici un point soulevé déjà dans son avis relatif au projet de loi sur la liberté d'expression dans les médias à propos du droit à l'information.

Article 9 paragraphe 1er lettre (c)

Proposition: – Supprimer le point (c) de l'article 9 et renuméroter les points subséquents.

– Ajouter un 2ème paragraphe avec la teneur suivante:

„Lorsque des données sont collectées directement auprès de la personne concernée, le responsable du traitement peut, par dérogation à l'article 26 paragraphe 1er, lettres (b) et (c), se limiter à indiquer la finalité générale poursuivie par le traitement mis en oeuvre aux seules fins de journalisme ou d'expression artistique ou littéraire.“

Commentaire:

Déjà dans son avis au sujet du projet de loi No 4910 sur la liberté d'expression dans les médias[19], la Commission a tenu à rendre attentif le gouvernement que l'exception de l'obligation d'informer la personne concernée du traitement de ses données à caractère personnel et de lui indiquer notamment la finalité poursuivie prévue à l'article 9 paragraphe 1er lettre (c) de la loi du 2 août 2002 déjà dans sa teneur actuelle pour l'hypothèse où l'application du principe général aurait pour conséquence de compromettre la collecte des données ou la publication peut déboucher sur une collecte déloyale de données (contraire à l'article 4 paragraphe 1er lettre (a)) dans l'hypothèse où les données sont recueillies directement auprès de la personne concernée.

La Commission nationale avait estimé que le texte actuel de l'article 9 paragraphe 1er lettre (c) qui devait être reproduit à l'article 68 de la loi sur la liberté d'expression dans les médias ouvrait grandement la porte à des abus et devait être modifié.

En effet, si en questionnant une personne sur des informations se rapportant à elle, à son comportement et à sa vie privée ou professionnelle, le journaliste n'aura pas à signaler qu'il recueille ces renseignements dans le cadre de son activité professionnelle et à des fins de publication, il y a de grands risques (et dans certains cas il pourra même se croire autorisé par la loi, voire encouragé à mentir délibérément) de voir la personne questionnée induite en erreur sur l'objet et le but de l'entretien de façon à l'inciter à faire des confidences qu'elle n'aurait pas faites si elle était consciente des fins envisagées par les questions de son interlocuteur. Une telle façon de procéder serait de toute évidence contraire à la bonne foi et à l'exigence du traitement loyal et licite des données à caractère personnel posé comme un des principes de base de la loi dont il n'y a pas de justification d'exempter les responsables de traitements effectués dans le cadre de la liberté d'expression (pas plus que d'autres) ce qui pourrait d'ailleurs être considéré comme une transposition incorrecte de la directive.

Cette proposition de texte est équilibrée et constitue un compromis entre les intérêts contradictoires existant en la matière:

– d'un côté, le responsable du traitement ne serait pas contraint d'indiquer avec précision les finalités déterminées, ou fournir d'autres informations supplémentaires (ce qui est le cas des traitements tombant sous le coup du droit commun inscrit à l'article 26 de la loi du 2 août 2002),

---

19 Délibération No 6bis/2003 du 17 octobre 2003 pages 16 à 18

– d'un autre côté, il devrait quand même informer la personne concernée qu'il entend opérer des traitements de données lui relatives aux seules fins de journalisme (ou d'expression artistique ou littéraire), ceci afin de minimiser d'emblée les risques d'abus.

Ainsi décidé à Luxembourg en date du 5 décembre 2005

La Commission nationale pour la protection des données,

Gérard LOMMEL	Pierre WEIMERSKIRCH	Thierry LALLEMANG
Président	*Membre effectif*	*Membre effectif*

*

ANNEXE 1

Tableau comparatif

Réglementations concernant les traitements de données à caractère personnel sur le lieu du travail dans les différents pays européens

(examen de 14 pays)

Pays	*Législation générale sur la protection des données à caractère personnel*	*Réglementation spécifique concernant la protection des données sur le lieu du travail*
Allemagne	– Loi fédérale du 14 janvier 2003 sur la protection des données (transposant la Directive 95/46/CE). – Deux lois de 1997 dans le secteur des télécommunications „Teledienstdatenschutzgesetz, TDDSG" et „Telekommunikationsgesetz, TKG"	Les lois TDDSG et TKG de 1997 contiennent des restrictions en matière de surveillance lorsque l'employeur permet l'usage des e-mails et d'Internet à des fins privées. La loi „Betriebsverfassungsgesetz" accorde aux représentants du personnel un droit de codécision sur les codes de conduites sur l'usage des e-mails et d'Internet à des fins privées et sur l'utilisation de moyens techniques destinés à surveiller le comportement et les performances des travailleurs.
Autriche	Loi fédérale de 2000 sur la protection des données (transposant la Directive 95/46/CE)	L'article 96 de la loi „Arbeitsverfassungsgesetz" prévoit l'accord obligatoire des organes de représentations du personnel pour l'installation de systèmes de surveillance susceptibles d'affecter la dignité des travailleurs.
Belgique	Loi du 8 décembre 1992, modifiée le 11 décembre 1998 sur la protection de la vie privée (transposant la Directive 95/46/CE)	– Convention collective de travail No 68 (16.6.1998) relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail – Convention collective de travail No 81 (26.4.2002) relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communications électroniques en réseau.

Pays	*Législation générale sur la protection des données à caractère personnel*	*Réglementation spécifique concernant la protection des données sur le lieu du travail*
Danemark	Loi du 31 mai 2000 sur le traitement des données à caractère personnel (transposant la Directive 95/46/CE)	La loi de 1982 sur la vidéosurveillance s'applique également à la surveillance sur le lieu du travail (information des salariés). Des dispositions du Code pénal relatives au secret des e-mails s'appliquent aux e-mails sur le lieu du travail.
Espagne	Loi du 13 décembre 1999 sur la protection des données (transposant la Directive 95/46/CE)	Le Code du travail soumet l'introduction d'un système de surveillance sur le lieu de travail à un avis préalable des organes de représentation du personnel.
Finlande	Loi du 22 avril 1999 sur la protection des données (transposant la Directive 95/46/CE)	Loi du 1er octobre 2001 sur la protection des données dans le contexte professionnel. Les représentants du personnel ont un droit de coopération en matière de surveillance et concernant l'usage des e-mails et d'Internet.
France	Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	Le Code du Travail dispose que les droits des personnes et les libertés individuelles et collectives ne peuvent pas être restreintes à moins que ce soit justifié par la nature de la tâche à accomplir et proportionné au but recherché. Obligation de l'employeur d'informer les salariés sur les traitements à des fins de surveillance.
Grèce	Loi de 1997 sur la protection des données (transposant la Directive 95/46/CE)	Une directive de l'autorité de contrôle interprète la loi-cadre sur la protection des données en vue de l'appliquer au contexte professionnel.
Irlande	Loi de 1988, modifiée en 2003, sur la protection des données (transposant la Directive 95/46/ CE)	/
Italie	Code de protection des données du 30 juin 2003 (transposant la Directive 95/46/CE)	Une loi (No 300/70) sur le statut des travailleurs interdit l'usage de moyens techniques (y compris les nouvelles technologies) en vue de contrôler les activités des travailleurs.
Pays-Bas	Loi du 6 juillet 2000 sur la protection des données (transposant la directive 95/46/CE)	Le consentement des organes de représentation du personnel est obligatoire en ce qui concerne l'usage des moyens de surveillance destinés à contrôler la présence, le comportement ou les performances des travailleurs (article 27.1 de la loi relative aux organes de représentation du personnel).
Portugal	Loi du 26 octobre 1998 sur la protection des données (transposant la Directive 95/46/CE)	La loi sur le contrat de travail réglemente indirectement la surveillance par l'employeur du contenu des e-mails des travailleurs et l'utilisation de l'Internet par ceux-ci.

Pays	*Législation générale sur la protection des données à caractère personnel*	*Réglementation spécifique concernant la protection des données sur le lieu du travail*
Royaume-Uni	Loi de 1998 sur la protection des données (transposant la Directive 95/46/CE)	Le „Regulation of Investigatory Powers Act“ de 2000 autorise les employeurs de surveiller et d'enregistrer des communications, sans le consentement des personnes concernées dans plusieurs hypothèses (p.ex. fournir la preuve d'une transaction commerciale; prévenir et détecter les crimes; rechercher ou détecter l'usage non autorisé du système de télécommunication).
Suède	Loi de 1998 sur la protection des données (transposant la Directive 95/46/CE)	La loi sur la codécision prévoit que d'importants changements sur le lieu de travail (y compris en matière de surveillance) doivent être négociés entre l'employeur et les syndicats.

*

ANNEXE 2

Résumé synthétique des législations des pays européens en matière de vidéosurveillance

1. *Dispositions spécifiques relatives à la vidéosurveillance contenues dans les différentes législations nationales sur la protection des données des pays membres*[20]

Selon les différents textes nationaux sur la protection des données, il apparaît que seulement le Luxembourg et le Portugal[21] ont spécifiquement prévu dans leurs lois respectives des obligations d'examen ou d'autorisation préalable par l'autorité de contrôle.

Ainsi ressort-il de l'article 14 (1) (a) de la loi luxembourgeoise du 2 août 2002 sur la protection des données à caractère personnel, qu'une autorisation préalable aux fins d'une vidéosurveillance doit obligatoirement être demandée auprès de la Commission nationale.

Il ressort de l'article 28 (1) (a) de la loi portugaise du 26 octobre 1998, renvoyant à l'article 8 paragraphe 2 de ladite loi qu'un contrôle préalable et donc une autorisation de la CNPD doit être obtenue pour un traitement de données relatif à „… des soupçons d'activités illicites, délits, infractions administratives, décisions infligeant des peines, mesures de sécurité, amendes et sanctions accessoires …“.

Il convient de noter que des autorisations préalables sont également nécessaires aux fins d'une vidéosurveillance en France, en Espagne et en Suède. Dans ces trois cas de figure, il s'agit cependant de textes spécifiques portant sur la vidéosurveillance exclusivement, ces dispositions ne découlent d'aucune façon de la législation sur la protection des données à caractère personnel.

En France, il faut une autorisation préalable de la préfecture du lieu d'installation du système de vidéosurveillance[22] afin de pouvoir opérer une vidéosurveillance (i) sur la voie publique ou (ii) dans les lieux ouverts au public.

En Espagne, il faut une autorisation préalable de l'administration des „forces et corps de sécurité“ pour toute installation d'un système de vidéosurveillance, par des personnes du secteur privé ou public.

En Suède, la vidéosurveillance „générale“ requiert en principe l'autorisation d'une commission administrative régionale[23], mais il existe cependant un certain nombre d'exceptions, p.ex. la sur-

20 L'examen ne porte pas sur les législations des pays suivants: Danemark et Irlande.

21 Ce point spécifique n'a pas pu être vérifié pour les pays suivants: Danemark et Irlande.

22 Loi No 95-73 du 21 janvier 1995 et décret No 96-926 du 17 octobre 1996

23 Loi 1998:150 relative à la vidéosurveillance générale

veillance des bureaux de poste, des banques et des magasins. La vidéosurveillance secrète (enquêtes criminelles) doit être autorisée par un tribunal[24].

Toutes les autres législations des pays membres ont prévu soit un mécanisme de déclaration préalable ou de notification préalable, soit elles sont muettes sur une telle mesure, tel p. ex. l'Allemagne.

2. *Le champ d'application des législations spécifiques sur la vidéosurveillance*

Les pays suivants se sont dotés de lois ou règlements spécifiques portant exclusivement sur la vidéosurveillance: l'Allemagne, le Danemark, l'Espagne, la France, les Pays-Bas, le Portugal, la Suède et l'Autriche. Il faut aussi citer l'Italie et le Royaume-Uni qui, à part les lois ou règlements spécifiques en la matière, ont également adopté des codes de conduite.

Les dispositions législatives spécifiques de l'Allemagne, l'Espagne, la France, la Suède et de l'Autriche ne portent que sur la vidéosurveillance dans des *lieux publics* (et parfois des *lieux ouverts au public*, cf. supra sur la France). Pour les autres pays, on est en présence de vidéosurveillances soit admises dans *les lieux privés et les lieux publics*, tels que l'Italie et le Royaume-Uni, les Pays-Bas[25], le Portugal, soit admises dans les *lieux privés*, tel que le Danemark (où les vidéosurveillances dans les lieux publics sont cependant admises sous conditions restrictives).

---

24 Loi 1995:1506 sur la vidéosurveillance secrète

25 Les vidéosurveillances privées sont admises, sous des conditions restrictives

Service Central des Imprimés de l'Etat