Jean-François LECLERCQ
David DE ROY
Jean-François NEVEN
Gilbert DEMEZ
Emmanuel PLASSCHAERT
Stanislas van WASSENHOVE
Eric CARLIER
Gaëtane ALBERT
Claude WANTIEZ

VIE PRIVÉE DU TRAVAILLEUR ET PRÉROGATIVES PATRONALES

Sous la direction scientifique de M. Jean-François LECLERCQ
Premier avocat près la Cour de cassation

ÉDITIONS DU JEUNE BARREAU DE BRUXELLES
2005

LA PROTECTION DES DONNÉES PERSONNELLES DANS LE CADRE DU CONTRÔLE DES PRESTATIONS DE TRAVAIL

par

Emmanuel PLASSCHAERT

Avocat
Crowell & Moring

A. OBSERVATIONS LIMINAIRES : LES TENSIONS NOUVELLES ENTRE PRÉROGATIVES PATRONALES ET RESPECT DE LA VIE PRIVÉE DES TRAVAILLEURS

La protection accrue de la vie privée de l'être humain est un sujet qui, ces dernières décennies, et plus particulièrement encore ces dernières années, est devenu une préoccupation majeure des instances législatives internationales, européennes et nationales et, dans la foulée des nouveaux textes normatifs mis en place, des instances créées pour surveiller les nouveaux principes et règles adoptés.

C'est dans ce contexte que la délicate question de l'équilibre entre le respect de la sphère privée du travailleur au temps et au lieu de travail et le pouvoir de surveillance et de contrôle de l'employeur est devenue plus aiguë.

Sans doute a-t-il toujours été admis, fût-ce implicitement, que le droit d'une personne au respect de sa vie privée ne s'éteignait pas au pas des portes de l'entreprise pour renaître une fois celles-ci franchies en

sens inverse [1]. L'équilibre entre les droits et obligations des employeurs et des travailleurs semble toutefois, pendant longtemps, avoir pu être assuré sur la base de l'arsenal législatif existant, les litiges en la matière étant relativement peu nombreux.

Parmi d'autres facteurs, le développement intense, ces dernières années, et la sophistication de plus en plus grande des nouvelles technologies ont toutefois mis en péril les anciennes solutions. Un autre phénomène récent, celui de l'effacement progressif des anciennes lignes de partage entre vie privée et vie professionnelle, également induit par les nouvelles technologies, a encore davantage accru ce risque de voir basculer l'équilibre précité en faveur de l'employeur [2].

Ce nouveau défi est ainsi parfaitement résumé par Monsieur l'avocat général M. Kehrig dans ses conclusions précédant l'arrêt de la Cour de cassation française (chambre sociale) du 2 octobre 2001 :

"'L'identité intime' du salarié qui n'est pas seulement un 'être de travail' doit en effet être respectée. Même sur les lieux du travail il a droit à une certaine autonomie car l'entreprise ne peut être un espace où l'arbitraire et le pouvoir discrétionnaire s'exercent sans frein, un 'terrain d'espionnage' où seraient bafoués les droits fondamentaux. Le tout numérique facilite le contrôle patronal mais une part, résiduelle, certes, mais irréductible de liberté de vie personnelle doit subsister dans l'entreprise alors, d'ailleurs, que le travail ou les impératifs nés du travail parasitent, plus ou moins, cette vie personnelle hors du temps et du lieu de travail." [3]

La redéfinition de règles du jeu plus précises et plus adaptées à l'environnement sociologique et technologique actuel est, dans ce contexte, devenue nécessaire et, à certains égards, urgente.

---

(1) Sans ambiguïté possible, et à plusieurs reprises, la Cour européenne des droits de l'homme a confirmé que le droit au respect de la vie privée et familiale, du domicile et de la correspondance, consacré par l'article 8 de la Convention européenne des droits de l'homme, s'appliquait également sur le lieu de travail et au temps de travail : Cour eur. D.H., arrêt Niemietz du 16 déc. 1992, *J.T.*, 1994, p. 65 ; arrêt Halford du 25 juin 1997, arrêt Amann du 16 févr. 2000, *www.echr.coe.int*; voir également Cass. fr., 2 octobre 2001, arrêt n° 4164, *www.courdecass.fr.*

(2) Voir à ce sujet les conclusions de Monsieur l'avocat général M. Kehrig précédant Cass. fr. (chambre sociale), 2 octobre 2001, arrêt n° 4164, *www.courdecassation.fr* et les références y citées.

(3) Cass. fr. (chambre sociale), 2 octobre 2001, arrêt n° 4164, *www.courdecassation.fr* et les références y citées.

Si les enjeux esquissés ci-dessus concernent tous les aspects de la vie privée du travailleur au temps et lieu de travail, la présente contribution s'attachera plus particulièrement à tenter de mieux cerner un de ceux-ci : le régime juridique applicable au traitement par l'employeur des données personnelles de ses travailleurs.

L'entreprise a de tout temps disposé de nombreuses données personnelles concernant ses travailleurs. Du point de vue de celle-ci, le traitement de ces données est susceptible de se justifier pour divers motifs légitimes : veiller à la sécurité du réseau informatique et se prémunir d'attaques informatiques, empêcher les diffusions électroniques de secrets d'affaires, optimaliser l'organisation du travail, contrôler la productivité des travailleurs, etc.

Indépendamment de ses raisons, liées aux nécessités de fonctionnement économiques, techniques ou commerciales de l'entreprise, s'ajoute la nécessité pour tout employeur de pouvoir traiter un certain nombre de données personnelles dans le cadre de la bonne gestion des ressources humaines et de l'administration des rémunérations.

Les nouvelles technologies ont non seulement permis de faciliter la gestion de ces données mais également d'étendre les capacités de contrôle de l'entreprise, qu'il s'agisse du type de données désormais susceptibles de faire l'objet d'un traitement ou du temps pendant lequel le contrôle peut être exercé.

Parallèlement à ce renforcement des capacités de gestion des données personnelles, le danger de voir l'entreprise s'immiscer trop profondément dans la sphère privée de ses travailleurs, soit, plus grave encore, recueillir ou utiliser, de quelque façon, des données à caractère personnel de façon illégitime est devenu bien plus tangible que par le passé.

De nombreuses dispositions légales et réglementaires ont été prises ces dernières années, au niveau international, européen et national pour répondre à ces dangers.

Nous examinerons ci-dessous plus particulièrement la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ("la loi du 8 décembre

1992"). Cette loi a été profondément modifiée en 1998 [4] en vue de transposer dans notre droit la directive n° 95/46 du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ("la directive"). Elle est complétée de mise en œuvre par l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard de traitements de données à caractère personnel [5] ("l'arrêté royal du 13 février 2001").

Bien que le champ d'application de ces textes légaux [6] dépasse, de loin, la sphère des relations de travail [7], ces dispositions contribuent à la redéfinition, évoquée ci-dessus, des règles du jeu régissant le précaire équilibre entre le droit légitime du travailleur au respect de sa vie privée et le droit tout aussi légitime de l'employeur d'exercer son pouvoir de surveillance et de disposer de toutes les informations nécessaires et utiles en vue de mener à bien une politique et une gestion des ressources humaines efficace.

B. LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL DES TRAVAILLEURS DE L'ENTREPRISE : GÉNÉRALITÉS

1. Observations liminaires

La loi du 8 décembre 1992 vise, de façon tout à fait générale, à garantir à toute personne physique [8], la protection de ses libertés et

---

(4) Loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *M.B.*, 3 févr. 1999, p. 3049 et suiv.

(5) Arrêté royal portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard de traitements de données à caractère personnel, *M.B.*, 13 mars 2001.

(6) Ce qui n'est au demeurant pas étranger aux difficultés d'application qu'ils peuvent susciter lors de leur mise en œuvre dans le contexte professionnel.

(7) Ils ne sont pas les seuls et d'autres lois, arrêtés ou conventions collectives de travail poursuivent, principalement ou incidemment, le même objectif ou complètent, en interférant parfois, ces dispositions dans des domaines spécifiques (contrôle de l'utilisation des messageries électroniques et de l'accès à Internet, surveillance par caméras). Ces dispositions sont examinées ailleurs dans cet ouvrage.

(8) Les données concernant les personnes morales ne sont donc pas protégées par la loi du 8 décembre 1992.

droits fondamentaux, notamment la protection de sa vie privée, lors du traitement de données à caractère personnel le concernant [9].

Le vaste monde des relations de travail est évidemment un terrain d'application privilégié de ces nouvelles dispositions, tant les traitements de données susceptibles d'être mis en œuvre par les entreprises sont nombreux et variés : gestion du dossier du travailleur, gestion des annuaires d'entreprises, organisation des élections sociales, administration des rémunérations, mise en place de systèmes de surveillance des courriels et de l'Internet, gestion des agendas professionnels, suivi des demandes de formations, etc.

Après avoir défini les principales notions mises en œuvre par la loi du 8 décembre 1992 et délimité son champ d'application, nous examinerons, du point de vue du contexte professionnel, les principes, obligations et droits des parties concernées, le régime applicable aux transferts de données hors Union européenne et les sanctions édictées par cette loi. L'objectif sera de tenter de mieux cerner les enjeux, les obligations et les droits qui en découlent pour l'entreprise et les travailleurs.

Transposant, depuis la loi modificative du 11 décembre 1998, la directive 95/46/CE du 24 octobre 1995, cette loi, destinée à s'appliquer à tout traitement de données personnelles, n'a pas été taillée sur mesure pour le monde de l'entreprise. Des notions aux contours parfois mal définis et certains mécanismes trop rigides ou contraignants, les interférences occasionnelles entre cette loi et les autres normes sociales applicables et, enfin, la nature particulière du rapport de subordination caractéristique de la relation de travail posent dès lors souvent des difficultés d'interprétation ou d'application. Nous y reviendrons plus concrètement ci-dessous, lorsque l'occasion se présente.

2. Les principales notions

L'article 1 du chapitre premier de la loi du 8 décembre 1992 est consacré à une liste de définitions des principales notions de la loi. Nous en examinons les principales.

---

(9) Art. 2 de la loi du 8 décembre 1992.

2.1. Les données à caractère personnel

Sont tout d'abord définies les *données à caractère personnel* [10], c'est-à-dire précisément celles que la loi vise à protéger. L'expression est très large puisqu'elle vise toute information relative à une personne physique identifiée ou identifiable. Cette personne est qualifiée par la loi de *personne concernée*. Est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

Il s'agira donc de données aussi diverses que le nom, le prénom et les coordonnées, l'état civil, les caractéristiques physiques, les opinions personnelles, les informations sur les activités passées, un examen médical, une empreinte digitale, etc.

L'exposé des motifs de la loi modificative du 11 décembre 1998 expose qu'une donnée personnelle tombe sous le champ d'application de la loi dès lors qu'il existe un moyen raisonnable d'identifier la personne à laquelle se rapportent les données, quand bien même le responsable du traitement ou le sous-traitant ne disposent pas de ce moyen [11].

Peu importe également le support utilisé : une image ou une bande sonore, par exemple, constituent également des données à caractère personnel au sens de la loi du 8 décembre 1992.

L'enjeu, dans les prochaines années, sera de déterminer plus concrètement quelles données sont protégées par la loi. Sans doute la discussion portera-t-elle notamment sur la nature personnelle ou non d'une donnée et sur le caractère raisonnable ou non de la possibilité de relier une information quelconque à une personne physique.

Le débat semble toutefois déjà sérieusement entamé comme l'illustre l'arrêt récent de la Cour de cassation du 2 mars 2005 considérant que *"la vidéosurveillance d'une caisse enregistreuse ne comporte, lorsqu'elle se limite à celle-ci, aucun élément d'identification*

---

(10) Loi du 8 déc. 1992, art. 1, § 1.

(11) Exposé des motifs, *Doc. Parl.*, Ch. Représ., sess. ord. 1997-1998, n° 1566/1 p. 12. L'exemple classique est celui du code ADN qui, quand bien même il serait entre les mains d'une personne n'ayant aucune connaissance génétique ni aucun appareillage lui permettant de le relier à son propriétaire, pourrait être considéré comme une donnée à caractère personnel.

directe ou indirecte, au sens de l'article 1er de la loi du 8 décembre 1992, de la personne qui l'emploie" [12].

Cette décision peut surprendre lorsqu'on sait qu'en l'espèce cette vidéosurveillance avait précisément été mise en œuvre afin de prendre en flagrant délit une caissière soupçonnée de vol. La possibilité de relier les images vidéo à la personne concernée était donc évidente mais la question, en amont, était celle de savoir si de simples images d'une caisse enregistreuse pouvaient ou non être considérées comme des données personnelles au sens de la loi. La Cour de cassation a tranché par la négative.

2.2. Le traitement

Les données à caractère personnel ne sont protégées par la loi du 8 décembre 1992 que pour autant qu'elles fassent l'objet d'un *"traitement"*. Par "traitement", on entend toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel [13].

Ici encore, l'expression revêt un sens très large, puisqu'elle vise en fait toute action ou ensemble d'actions effectué sur des données à caractère personnel. La définition du traitement a pour conséquence pratique que des opérations extrêmement banales et ne présentant guère de risque pour la personne concernée sont susceptibles de se voir appliquer la loi.

---

(12) Cass., 2 mars 2005, P.04.1644.F/8, *www.juridat.be*. Cet arrêt, qui admet par ailleurs la possibilité pour un juge, dans le cadre d'une procédure pénale, de ne pas écarter des éléments de preuve irrégulièrement recueillis est par ailleurs analysé, dans le présent ouvrage, par M. Jean-François Neven et Me Claude Wantiez, notamment quant à la question cruciale de la transposition éventuelle de cet enseignement au plan civil.

(13) Art. 1, § 2, loi du 8 déc. 1992.

2.3. Les divers intervenants concernés

La loi du 8 décembre 1992 s'attache ensuite à envisager les diverses catégories de personnes susceptibles d'être impliquées dans le traitement de données à caractère personnel.

Elle définit ainsi tout d'abord le *responsable du traitement* [14]. Par *"responsable du traitement"*, la loi entend la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel [15]. Ainsi que le laisse supposer son appellation, le responsable du traitement est le premier concerné par la loi qui fait peser sur lui la grande majorité des obligations qu'elle instaure [16]. Dans le contexte professionnel, le responsable du traitement sera généralement l'employeur.

La loi prévoit la possibilité d'une action conjointe de plusieurs responsables du traitement. Ce sera par exemple le cas lorsque diverses sociétés d'un même groupe déterminent ensemble les finalités et les moyens d'un traitement.

Le responsable du traitement sera bien souvent une personne morale, comme une entreprise ou une administration qui, après avoir pris l'initiative du traitement, en confiera le traitement à une tierce personne physique ou morale. La loi du 8 décembre 1992 prévoit cette situation et qualifie de sous-traitant [17] la personne qui se verra ainsi confier la tâche de traiter, pour le compte du responsable du traitement, les données à caractère personnel. Dans le contexte professionnel

---

(14) Art. 1, § 4, al. 1er, loi du 8 déc. 1992.

(15) Des problèmes pratiques risquent de se poser, notamment au sein des grands groupes de sociétés, lorsque la détermination des finalités se fait dans le chef d'une entité tandis que la détermination des moyens se fait dans le chef d'une autre, puisque les critères légaux sont *a priori* cumulatifs. De l'exposé des motifs de la loi, il apparaît que l'important, dans un tel cas, sera d'identifier celui qui décide des finalités du traitement. Le critère relatif aux finalités prévaut donc sur celui relatif aux moyens.

(16) Y. POULLET et Th. LEONARD, "La protection des données à caractère personnel en pleine (r)évolution – La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995", *J.T.*, 1999, p. 379.

(17) Art. 1, § 5, loi du 8 déc. 1992. Par "sous-traitant", on entend la personne physique ou morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données. Un travailleur agissant sous l'autorité de son employeur n'est donc pas un sous-traitant.

l'exemple type est bien entendu celui du secrétariat social chargé du calcul des rémunérations [18].

Le destinataire, enfin, est la personne physique ou morale, l'association de fait ou l'administration publique qui reçoit communication des données, qu'il s'agisse ou non d'un tiers [19].

Enfin, toutes les personnes physiques ou morales qui pourraient intervenir dans le processus sans entrer dans les catégories précitées sont qualifiées de tiers [20]. Les qualités de tiers et de destinataires ne sont pas incompatibles, en ce sens que le destinataire peut très bien être en même temps un tiers. Il suffit qu'il reçoive communication des données à caractère personnel et qu'il ne fasse pas partie d'une des catégories précitées.

3. Champ d'application

3.1. Rationae materiae et personae

3.1.1 Le principe

La protection légale vise à garantir les libertés et droits fondamentaux, notamment le respect de la vie privée des personnes physiques, à l'occasion de tout traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un *fichier* [21].

En d'autres termes, toute action opérée sur des informations relatives à une personne physique tombe *a priori* sous le coup de la loi,

---

(18) Th. LEONARD, "La protection des données à caractère personnel et l'entreprise", *Guide juridique de l'entreprise*, t. XI, L. 112.1, Kluwer, 2e éd. 2004.

(19) Les instances administratives ou judiciaires qui sont susceptibles de recevoir communication des données dans le cadre d'une enquête particulière ne sont toutefois pas considérées comme des destinataires (art. 1, § 7, loi du 8 déc. 1992).

(20) Il s'agit, aux termes de la loi, de la personne physique ou morale, de l'association de fait ou administration publique, autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données (art. 1, § 6, loi du 8 déc. 1992).

(21) Loi 8 déc. 1992, art. 2 et 3, § 1. Par "fichier", on entend tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique (art. 1, § 3, loi du 8 déc. 1992)

pour autant que l'action en question soit automatisée, en tout ou en partie ou, si elle est manuelle, que les données soient organisées en un fichier et donc accessibles selon des critères logiques, comme par exemple l'ordre alphabétique.

Il convient de noter ici que la Commission de la protection de la vie privée ("la Commission") [22], interprète très largement la notion de fichier puisqu'elle considère que des archives conservées "en bon ordre" peuvent constituer des fichiers, sous réserve de l'analyse *in concreto* des circonstances de l'espèce [23]. Les traitements purement manuels figurant dans un fichier font toutefois l'objet de moins d'attention de la loi, les traitements automatisés étant bien plus réglementés [24].

Eu égard à l'objectif de protection des libertés et droits fondamentaux expressément énoncé à l'article 2 de la loi du 8 décembre 1992, la question fondamentale qu'il est ici permis de se poser est celle de la légitimité de la détermination des limites du champ d'application *ratione materiae* de la loi par référence à ses objectifs avoués.

Ne pourrait-on soutenir que la loi ne trouvera à s'appliquer que lorsqu'un traitement est spécifiquement et volontairement mis en œuvre en vue du traitement de données personnelles et non pas lorsque le traitement de données personnelles ne survient qu'incidemment, involontairement ou accidentellement en quelque sorte, ou encore est mis en œuvre dans des circonstances exceptionnelles.

Ainsi, la mise en place par une entreprise de procédés de surveillance, par exemple par vidéosurveillance, des entrepôts ou autres locaux de rangement dans lesquels les travailleurs ne sont pas occupés (et ou, au demeurant, personne n'est supposé circuler quand le système de vidéosurveillance est actif), peut-il être considéré comme un traitement par la loi du 8 décembre 1992 eu égard aux objectifs

---

(22) La Commission est un organe indépendant, institué auprès de la Chambre des représentants, chargé de la mise en œuvre et de la surveillance de la loi du 8 décembre 1992. Nous reviendrons ci-dessous sur le rôle de cet important rouage dans le cadre du système de protection des données à caractère personnel mis en place par la loi.

(23) Avis n° 15/2000 du 24 mai 2000, *www. privacy.fgov.be.*

(24) La notion de traitement automatisé n'est pas définie mais elle vise une réalité très large englobant presque toutes les nouvelles technologies de l'information, telles que l'informatique, les réseaux de télécommunication, etc. Voyez Th. LEONARD, "La protection des données à caractère personnel et l'entreprise", *op. cit.*, p. 14. Cet auteur précise que le procédé doit recourir à une machine "intelligente", ce qui exclut les photocopieuses et les téléfax.

poursuivis par celle-ci ? Une personne ayant pénétré, de façon illégitime, dans lesdits entrepôts ou locaux pourrait-t-elle invoquer à son bénéfice le non-respect éventuel par l'entreprise des dispositions de la loi au seul prétexte que la caméra l'a enregistré et donc que des données personnelles (images) ont été traitées [25] ?

Une interprétation téléologique de la loi du 8 décembre 1992 nous semble donc souhaitable si on veut éviter les conséquences par trop absurdes d'une interprétation textuelle de celle-ci dans des circonstances telles que décrites ci-dessus.

3.1.2 Les exceptions

De nombreuses exceptions figurent dans le texte légal. Elles portent tantôt sur l'entièreté de la loi, tantôt sur certaines de ses dispositions. Aucune ne concernant le monde de l'entreprise, nous ne les examinerons pas.

3.2. Rationae loci

La question du champ d'application territorial est l'une des plus délicates que pose la loi du 8 décembre 1992. En raison des nombreuses catégories d'intervenants potentiels prévus par la loi, du fait que ceux-ci peuvent être physiquement établis dans plusieurs pays différents et de l'inspiration européenne de la loi, il n'est pas toujours évident de définir le champ d'application *ratione loci* de celle-ci. Ce problème se rencontrera très fréquemment en matière de relations de travail, dans le cas notamment des grands groupes mondiaux disposant de nombreuses filiales ou succursales en Europe. Quel est à ce moment le critère de rattachement à prendre en considération pour apprécier l'applicabilité de la loi belge ? Il convient de distinguer selon que le responsable du

---

(25) La Cour de cassation française a déjà eu l'occasion de se prononcer à cet égard et a estimé que l'employeur est libre de mettre en place des procédés de surveillance (en l'espèce une vidéosurveillance) des entrepôts ou autres locaux de rangement dans lesquels les salariés ne travaillent pas (Cass. fr., 31 janvier 2001, Bull. V, n° 28). La Cour s'est toutefois uniquement prononcée sur la violation de l'article L. 432-2-1 du Code du travail français qui dispose que le comité d'entreprise est informé et consulté préalablement à toute décision de mise en œuvre dans l'entreprise de moyens ou techniques permettant un contrôle de l'activité des salariés. En l'espèce, la Cour a donc estimé que cette disposition était inapplicable en cas de mise en place des procédés de surveillance des entrepôts ou autres locaux de rangement dans lesquels les salariés ne travaillent pas. Un raisonnement similaire pourrait être adopté pour justifier la non-application des dispositions de la loi du 8 décembre 1992 dans une telle hypothèse.

traitement ait ou non un établissement sur le territoire de l'Union européenne.

3.2.1. Le responsable du traitement a un établissement sur le territoire de l'Union européenne

Selon son article 3 *bis*, 1°, la loi s'appliquera à *"tout traitement effectué dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge ou en un lieu où la loi belge s'applique en vertu du droit international public"*. Il suffit donc qu'un traitement soit effectué *dans le cadre* des activités d'un établissement situé en Belgique, quelle que soit sa forme juridique, pour que la loi s'applique à ce traitement. Par conséquent, un traitement pourrait très bien être soumis à la loi belge alors qu'il ne serait pas effectué en Belgique : il suffit qu'il ait lieu dans le cadre des activités de l'établissement. Ainsi la gestion d'une base de données concernant le personnel d'une entité située en Belgique mais assurée à l'étranger tombera-t-il en principe sous l'application de la loi belge.

La règle paraît claire, mais encore faut-il pouvoir déterminer quand un traitement doit être considéré comme intervenant dans le cadre des activités d'un établissement. Selon certains auteurs, il faut considérer qu'une participation de l'établissement au traitement des données est nécessaire pour que la loi s'applique. Il ne suffirait donc pas que ce traitement lui profite simplement. Ainsi par exemple, le fait qu'une société dispose d'un accès on line à une banque de données organisée dans un autre pays par une société liée n'entraînera pas l'application à cette société de la loi belge. Il en irait autrement si cette société effectuait elle-même un traitement des données, par exemple, en les intégrant dans sa propre base de données [26].

Cette interprétation [27] permettrait de considérer qu'un traitement, la gestion d'un plan d'options sur action par exemple, poursuivi dans le cadre des activités d'un groupe de sociétés établies dans différents pays européens mais centralisé auprès de l'une d'entre elles ne serait soumise qu'à la loi nationale de la société qui poursuit le traitement, à moins que les autres sociétés non seulement bénéficient du traitement centralisé mais participent également à ce traitement.

---

(26) En ce sens : Th. LEONARD, *op. cit.*, p. 23, n° 249; Th. LEONARD et Y. POULLET, *op. cit.*, p. 383, n° 20. Les auteurs se fondent sur les travaux préparatoires de la loi modificative du 11 décembre 1998.

(27) Th. LÉONARD et Y. POULLET, *op. cit.*, p. 382 n° 19.

Enfin, lorsque le responsable du traitement exerce des activités sur le territoire de plusieurs États membres de l'Union européenne, il doit selon la Commission *"s'assurer que chacun des établissements dont il est responsable remplit les obligations prévues par le droit national du pays dans lequel les activités s'effectuent"* [28].

3.2.2. Le responsable du traitement n'a pas d'établissement sur le territoire de l'Union européenne

L'article 3 *bis*, 2°, de la loi envisage le cas où le responsable du traitement est situé en dehors de l'Union européenne et traite des données en faisant appel à des moyens situés en Belgique, exception faite des moyens utilisés à des seules fins de transit [29]. Le responsable du traitement devra alors désigner un représentant établi sur le territoire belge [30]. Les moyens dont il est ici question visent une réalité très large englobant tous les modes matériels de traitement comme les ordinateurs, les unités d'impression, les appareils de télécommunication, etc. [31].

4. Les principes clés régissant tout traitement de données à caractère personnel et les régimes particuliers

Lorsqu'un traitement de données à caractère personnel relève du champ d'application matériel, personnel et territorial de la loi du 8 décembre 1992, la licéité de celui-ci dépendra du respect d'un certain nombre de principes clés. L'entreprise est, en outre, soumise à diverses obligations visant à assurer une protection effective et adéquate des personnes concernées.

Nous examinerons sous ce point les principes clés. Les obligations à charge des intervenants concernés seront, pour autant qu'elles soient pertinentes du point de vue de la gestion des ressources humaines, examinées sous le point suivant.

---

(28) *http://www.privacy.fgov.be/declarations/lexique1.htm.*

(29) Lorsque le responsable du traitement n'est pas établi de manière permanente sur le territoire de la Communauté européenne et recourt, à des fins de traitement de données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire belge, autres que ceux qui sont exclusivement utilisés à des fins de transit sur le territoire belge (loi du 8 déc. 1992, art. 3 *bis*, 2°, al. 1er).

(30) Loi du 8 déc. 1992, art. 3 *bis*, 2°, al. 2.

(31) Exposé des motifs, p. 27.

4.1. Régime général

Tout traitement de données à caractère personnel doit toujours répondre aux principes clés énumérés ci-dessous. Si ces principes sont respectés, le traitement pourra être mis en œuvre sous réserve du respect des mesures de protection pratiques qui seront examinées ultérieurement sous le point suivant.

4.1.1. Le traitement doit être licite et loyal

Le traitement, en d'autres termes, devra respecter toutes les conditions prévues par la loi du 8 décembre 1992 et respecter le principe de transparence. Ce dernier est un principe très important. Il constitue en quelque sorte la première garantie de nature procédurale dont doit bénéficier toute personne concernée par un traitement de ces données personnelles.

Ce principe implique que la personne concernée soit clairement informée de l'existence et des raisons d'un traitement. Le respect de ce principe conditionnera sa capacité à exercer, le cas échéant, de façon effective les autres droits qui lui sont reconnus par la loi du 8 décembre 1992. Il est à cet égard étonnant de constater qu'il n'existe, contrairement à ce qui est notamment le cas en France ou en Allemagne, aucune disposition légale ou réglementaire prévoyant une procédure d'information et de consultation spécifique des instances représentatives du personnel. Le conseil d'entreprise est certes appelé à intervenir dans le cadre de l'introduction de nouvelles technologies [32] ou préalablement à la mise en œuvre d'un système de surveillance par caméra [33] ou de contrôle des données de communication électroniques en réseau [34] mais il ne semble pas avoir reçu expressément une mission d'information et de consultation générale concernant la mise en œuvre au sein de l'entreprise de traitements de données concernant le personnel.

---

(32) Convention collective de travail n° 39 concernant l'information et la concertation sur les conséquences sociales de l'introduction de nouvelles technologies (A.R. du 25 janvier 1984, *M.B.*, 8 févr.)

(33) Convention collective de travail n° 68 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail (A.R. du 20 sept., *M.B.*, 2 oct.)

(34) Convention collective de travail n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communications électroniques en réseau (A.R. du 21 juin, *M.B.*, 29 juin)

Deux décisions du 26 mai 2005 de la Commission nationale de l'informatique et des libertés (CNIL) [35], autorité administrative indépendante chargée de veiller à la protection des données personnelles en France, illustrent de façon particulièrement éloquente l'importance que revêtent ces exigences de licéité et de loyauté.

La CNIL a refusé d'autoriser [36] la mise en œuvre de dispositifs de "lignes éthiques" au sein de deux entreprises, filiales de sociétés américaines cotées. Ces dispositifs étaient destinés à permettre aux travailleurs de l'entreprise de signaler des comportements supposés fautifs imputables à leurs collègues de travail. La mise en œuvre de tels dispositifs est imposée par la loi américaine Sarbanes-Oxley. Celle-ci oblige toute entreprise cotée au New York Stock Exchange (NYSE) ou au Nasdaq à mettre en place des procédures permettant aux salariés de rapporter, de façon anonyme, à leur employeur toute malversation financière ou comptable. Le non-respect de cette obligation peut entraîner des sanctions importantes pour l'entreprise concernée.

La CNIL a estimé que la mise en œuvre par un employeur d'un dispositif destiné à organiser auprès de ses travailleurs le recueil, quelle qu'en soit la forme, de données personnelles concernant des faits contraires aux règles de l'entreprise ou à la loi imputables à leurs collègues de travail, en ce qu'il pourrait conduire à un système organisé de délation professionnelle, ne pouvait qu'appeler de sa part une réserve de principe au regard de la loi française du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

La CNIL a également jugé que le dispositif était disproportionné au regard des objectifs poursuivis et des risques de dénonciations calomnieuses et de stigmatisation des employés objets d'une "alerte éthique". Elle a enfin relevé que les modalités de collecte et de traitement de ces données, dont certaines pourraient concerner des faits susceptibles d'être constitutifs d'infractions pénales, ne pouvaient être considérées comme loyales au sens de l'article 6 de la loi du 6 janvier 1978 précitée [37].

---

(35) Délibérations n° 2005-110 et n° 2005-111, *www.cnil.fr*.

(36) En France, certains traitements sont non seulement soumis à une procédure de déclaration auprès de la CNIL mais également à un régime d'autorisation préalable.

(37) Ces décisions ont provoqué l'inquiétude des entreprises concernées qui, quoi qu'elles fassent, sont exposées au risque de sanctions conséquentes. Si elles passent outre le refus de la CNIL, elles s'exposent à des sanctions pénales en France. Si elles ne mettent pas en œuvre le dispositif requis, elles courent en revanche le risque de voir les autorités

À notre connaissance, la Commission n'a, à ce jour, pas encore pris position en la matière en Belgique.

4.1.2. Les données doivent être collectées pour des finalités déterminées, explicites et légitimes

Le principe de finalité implique que les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage légitime. La collecte de données à caractère personnel pourra se faire pour plusieurs finalités distinctes, mais elles devront toutes être légitimes.

La loi se borne à énoncer le principe sans définir davantage les finalités susceptibles d'être considérées comme légitimes. En prévoyant toutefois, à l'article 5, de façon exhaustive les cas dans lesquels un traitement peut avoir lieu, elle détermine indirectement les finalités *a priori* légitimes. Parmi ces cas, les suivants présentent un intérêt au regard des relations entre employeur et travailleurs :

- la personne concernée a donné son consentement ;

  L'employeur qui collecte des données à caractère personnel auprès de ses travailleurs et qui ne peut se fonder sur aucune des autres hypothèses légales devra donc obtenir – et être en mesure de prouver – le consentement des travailleurs concernés.

  Pour être valable, le consentement devra consister en une manifestation de volonté libre, spécifique et informée de la personne concernée ou de son représentant légal par laquelle celle-ci accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement [38].

  La question du consentement dans le cadre des relations de travail pourrait, dans certains cas particuliers, s'avérer problématique en raison du rapport hiérarchique existant entre les parties en cause. En règle, nous pensons cependant qu'il n'y a pas lieu de considérer que cette seule circonstance serait de nature à vicier le consentement requis au sens de l'article 5 de la loi. Il n'y a évidemment aucun problème lorsque le consentement est donné lors de la conclusion du

---

boursières américaines sanctionner le non-respect des dispositions de la loi Sarbanes-Oxley. Il semble toutefois qu'un processus d'information et de discussion concernant cette question ait été engagé entre les autorités américaines et européennes compétentes (la problématique n'étant pas spécifique à la France mais concernant tous les pays de l'Union européenne).

(38) Loi du 8 déc. 1992, art. 1, § 8.

contrat de travail. Dans la plupart des cas, la question ne se posera d'ailleurs pas, le traitement étant susceptible d'être autorisé sur une autre base juridique ;

- le traitement est nécessaire à l'exécution du contrat (de travail) ou à l'exécution de mesures précontractuelles prises à la demande du (candidat) travailleur.

  Il s'agit évidemment de l'hypothèse que l'on rencontrera le plus souvent dans le contexte professionnel et qui permettra à l'entreprise de justifier *a priori* tel ou tel traitement de données ;

- le traitement est nécessaire au respect d'une obligation à laquelle l'entreprise est soumise par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

De manière générale, on pourrait ainsi citer la bonne tenue des divers documents sociaux, la retenue des cotisations de sécurité sociale ou du précompte professionnel...

4.1.3. Les données ne peuvent être traitées ultérieurement de manière incompatible avec les finalités en vue desquelles elles ont été originellement collectées [39]

Les données ne peuvent être traitées ultérieurement de manière incompatible avec les finalités en vue desquelles elles ont été originellement collectées, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables.

La Commission a ainsi déjà estimé que la photo d'un employé prise en vue de la confection d'un badge d'identification ne pouvait pas figurer sur un site intranet ni apparaître sur une brochure éditée par l'employeur sauf accord explicite de l'employé pour ces autres finalités [40].

Le critère décisif sera ici bien souvent celui des prévisions raisonnables de l'intéressé quant aux éventuelles autres finalités compatibles avec celles qui lui furent communiquées lors de la collecte originelle des données concernées. Cette exigence signifie *a contrario* que les données pourraient être traitées pour des finalités différentes de

---

(39) La loi prévoit une exception, à savoir le traitement ultérieur à des fins historiques, statistiques ou scientifiques.

(40) Avis n° 2/2004 du 26 févr. 2004, *www.privacy.fgov.be.*

celles qui ont présidé à leur collecte pour autant que les finalités nouvelles soient compatibles avec les finalités originelles.

Si, en revanche, les nouvelles finalités envisagées sont incompatibles avec les finalités initiales, il faut considérer qu'il y a nouveau traitement. Ceci entraînera l'obligation de vérifier à nouveau si ce nouveau traitement répond aux principes clés et, le cas échéant, d'exécuter les diverses obligations applicables.

Cette exigence pourrait notamment s'avérer problématique en cas restructuration de l'entreprise impliquant une cession éventuelle de tout ou partie de l'entreprise. Préalablement à toute opération de ce genre, le candidat repreneur exigera généralement de pouvoir procéder à un audit juridique – une procédure de due diligence – impliquant la mise à disposition du candidat repreneur d'un certain nombre d'informations relatives aux permis, contrats, brevets... et personnel de l'entreprise.

L'entreprise concernée pourra-t-elle alors communiquer au candidat repreneur les informations jadis collectées, par exemple, en vue de la gestion du personnel ? Les travailleurs peuvent-ils raisonnablement prévoir que des données comme leur date de naissance, leur date d'entrée en service, leur rémunération et avantages divers... nécessaires à la gestion des ressources humaines peuvent également être utilisées en vue de permettre à un candidat à la reprise de la société d'apprécier l'opportunité, les risques... d'une telle acquisition ?

À notre connaissance, la Commission ne s'est pas encore prononcée à cet égard. En revanche, la *Registratiekamer* néerlandaise a eu à connaître de cette problématique et a considéré qu'une telle finalité était incompatible avec la finalité initiale de gestion du personnel [41].

4.1.4. Les données doivent être adéquates, pertinentes et non excessives

Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.

La Commission a ainsi estimé qu'en application de ce principe le badge confié par l'entreprise au travailleur pour surveiller ses

(41) Voir avis de la Registratiekamer du 2 novembre 1998 – 98vo525.2, *www.registratiekamer.nl.*

déplacements ne doit pas mentionner les nom et prénom du travailleur, mais uniquement sa photo et un numéro d'identification [42].

Nous verrons ci-dessous que cette exigence permet également résoudre la question de l'équilibre à trouver entre la prérogative patronale de contrôle et le respect de la vie privée du travailleur en matière de géolocalisation.

4.1.5. Les données doivent être exactes et, si nécessaire, mises à jour

Les données doivent être exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables doivent être prises afin que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées, soient effacées ou rectifiées [43].

4.1.6. Les données ne peuvent être conservées que pendant une durée raisonnable

Les données doivent être conservées sous une forme qui permet d'identifier les personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités du traitement.

4.2. Régime dérogatoire : le cas du traitement des données sensibles

4.2.1. Les principes applicables

Si les conditions qui viennent d'être examinées sont remplies, le traitement des données à caractère personnel est en principe permis. Néanmoins, s'agissant de certains types de données de nature particulière, le législateur a inversé le principe en prévoyant une interdiction de principe assortie toutefois de nombreuses exceptions. C'est le régime des données sensibles, parmi lesquelles la loi distingue trois catégories.

---

(42) Avis n° 2/2004 du 26 févr. 2004, *http://www.privacy.fgov.be.*

(43) Loi du 8 déc. 1992, art. 4, § 1, 4°.

(i) Les données sensibles stricto sensu

Les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que les données relatives à la vie sexuelle ne peuvent en règle faire l'objet d'un traitement [44]. Il s'agit des données sensibles *sensu stricto*.

Dans le contexte professionnel, on songe à des données se rapportant à des demandes de congés pour raisons religieuses (communions, mariages...), des primes syndicales...

Parmi les nombreuses exceptions prévues, il y a tout d'abord le cas dans lequel la personne concernée a donné son consentement, pour autant que celui-ci ait été donné par écrit et soit révocable *ad nutum*. Signalons toutefois une exception à cette exception lorsque le responsable du traitement est l'employeur présent ou potentiel de la personne concernée ou lorsque la personne concernée se trouve dans une situation de dépendance vis-à-vis du responsable du traitement qui l'empêche de refuser librement son consentement [45]. Dans un tel cas, le consentement, même écrit, même révocable à tout instant, ne suffira pas à autoriser le traitement de données sensibles concernant les travailleurs de l'entreprise sauf lorsque le traitement vise à octroyer un avantage à la personne concernée [46].

L'entreprise peut également faire valoir que le traitement est nécessaire afin d'exécuter les obligations et droits spécifiques en matière de droit du travail ou encore démontrer que le traitement porte sur des données manifestement rendues publiques par la personne concernée ou enfin qu'il est nécessaire à la réalisation d'une finalité fixée par ou en vertu de la loi en vue de l'application de la sécurité sociale [47].

(ii) Les données relatives à la santé

Est également interdit le traitement des données relatives à la santé. Comme pour la précédente interdiction, certaines dérogations

---

(44) Loi du 8 déc. 1992, art. 6, § 1.

(45) A.R. 13 févr. 2001, art. 27. Cette exception à l'exception est également applicable aux données relatives à la santé.

(46) Le consentement écrit de travailleurs permettrait par exemple à l'employeur de collecter et traiter des données relatives à leurs convictions religieuses s'il le fait dans le but de mettre à leur disposition un lieu de culte.

(47) Loi du 8 déc. 1992, art. 6, § 2.

existent. Les garanties qui doivent accompagner celles-ci sont toutefois encore plus sévères [48].

(iii) Les données judiciaires

Est enfin interdit le traitement des données relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté [49].

Une des rares dérogations à l'interdiction de traitement de données judiciaires susceptibles de présenter un intérêt pour un employeur est celle concernant le traitement de ce type de données lorsque celui-ci est nécessaire à la réalisation de finalités fixées par ou en vertu d'une loi, d'un décret ou d'une ordonnance [50]. Faisant application de ces règles, la Commission a ainsi estimé que *"les agences de placement ne sont légalement pas autorisées à conserver, reproduire ou transmettre le certificat de bonnes vies et mœurs des candidats inscrits auprès d'elles, sauf dans les cas où des dispositions légales obligent l'utilisateur à vérifier les antécédents judiciaires du travailleur"* [51].

(48) Loi du 8 déc. 1992, art. 7, § 1 et 2. En ce qui concerne la problématique particulièrement complexe des informations médicales dans le contexte professionnel, voir N. HAUTENNE, K. ROSIER et S. GILSON, "Les informations médicales dans la relation de travail", *Or.*, Numéro spécial contenant les actes du colloque du 10 mars 2005 relatif à l'employeur et la vie privée au travail.

(49) Loi du 8 déc. 1992, art. 8.

(50) Loi du 8 déc. 1992, art. 8, § 2, b).

(51) Avis n° 08/2002 du 11 févr. 2002 relatif au traitement de données à caractère personnel réalisé par les sociétés privées d'intérim, *www.privacy.fgov.be.*

4.2.2. Les conditions spécifiques applicables au traitement de données sensibles [52]

Le traitement des données sensibles doit non seulement respecter les principes clés définis ci-dessus mais est, en outre, soumis, à des conditions supplémentaires, à caractère principalement organisationnel et contractuel. La loi a laissé au Roi le soin de déterminer celles-ci, ce que celui-ci a fait aux articles 25 à 27 de l'arrêté royal du 13 février 2001. Nous nous permettons d'y renvoyer [53].

5. Les obligations de l'entreprise et les droits des personnes concernées

L'entreprise [54] est soumise à diverses obligations visant à assurer une protection effective et adéquate des personnes concernées. Celles-ci peuvent être divisées en trois catégories principales : obligation d'information de la personne concernée, obligation de mise en place de mesures permettant d'assurer la confidentialité et la sécurité du traitement et, enfin, obligation de déclaration du traitement à la Commission.

5.1. L'obligation d'information de la personne concernée

Tout personne concernée par un traitement de ses données personnelles doit spontanément recevoir un certain nombre d'informations au moment où celles-ci sont collectées par l'entreprise [55]. La loi entend ainsi garantir la transparence du traitement des données à caractère personnel à l'égard de la personne concernée.

Il est intéressant de constater que la loi du 8 décembre 1992 ne prescrit pas la forme que doit emprunter l'information [56]. Elle peut par conséquent parfaitement être verbale. Il est clair toutefois qu'en vue de se réserver une preuve du respect de ses obligations, l'entreprise aura

---

(52) A.R. du 13 févr. 2001, art. 25 à 27.

(53) Pour plus de détails, voir E. PLASSCHAERT et J.-A. DELCORDE, "Le traitement et la protection des données personnelles des travailleurs", *Or.*, Numéro spécial contenant les actes du colloque du 10 mars 2005 relatif à l'employeur et la vie privée au travail.

(54) Nous supposons, dans le cadre de l'énumération des obligations à charge du responsable du traitement que c'est bien l'entreprise qui doit être considérée comme telle.

(55) Loi du 8 déc. 1992, art. 9.

(56) Certaines réglementations spécifiques prévoient ou suggèrent toutefois les formes selon lesquelles certaines informations, le cas échéant complémentaires à celles prévues par la loi du 8 décembre 1992, doivent être communiquées.

tout intérêt à procéder à une information écrite, le cas échéant sous forme électronique [57]. Dans un contexte professionnel, la plupart des informations usuelles pertinentes dans le cadre de la gestion des ressources humaines seront généralement collectées à l'occasion de la conclusion du contrat de travail. Le plus simple consistera donc à insérer dans le contrat de travail une clause spécifique à cet égard.

La loi distingue les deux situations qui peuvent se présenter en pratique en matière de collecte de données : soit les données sont directement recueillies auprès de la personne concernée, soit elles sont transmises par un tiers.

5.1.1. Hypothèse où les données sont collectées auprès de la personne concernée

Dans la première hypothèse, c'est au plus tard au moment de la collecte des données que l'entreprise doit donner à la personne concernée les informations suivantes, sauf si la personne concernée en est déjà informée [58] :

- le nom et l'adresse de l'entreprise et, le cas échéant, de son représentant ;
- les finalités du traitement ;
- les informations supplémentaires suivantes, sauf dans les cas où cela n'est pas nécessaire pour garantir le caractère loyal du traitement des données [59] :
  - les destinataires ou les catégories de destinataires des données ;
  - le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse ;
  - l'existence d'un droit d'accès et de rectification des données la concernant (voir ci-dessous).

---

(57) L'objet de la preuve étant ici un fait juridique, il peut être prouvé par toutes voies de droit, témoignages et présomptions compris, mais le mode le plus sûr demeure évidemment la preuve écrite.

(58) Nous ne reprenons ici que les seules informations pertinentes dans le cadre du contexte professionnel.

(59) Loi 8 déc. 1992, art. 9, § 1, d).

5.1.2. Hypothèse où les données sont collectées auprès d'un tiers

Dans la seconde hypothèse, l'entreprise devra fournir les mêmes informations [60]. Elle devra, en outre, communiquer les catégories de données concernées [61].

Ces informations devront être communiquées au moment de l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données à des tiers.

Dans cette seconde hypothèse, les cas de dispense à l'obligation d'information de la personne concernée prévus dans la première hypothèse sont repris, mais la loi prévoit également quelques dispenses complémentaires. Ainsi, l'information ne devra pas être communiquée lorsque l'enregistrement ou la communication des données est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

5.2. Les droits d'accès, de rectification et d'opposition de la personne concernée

La personne concernée se voit reconnaître par la loi du 8 décembre 1992 un droit d'accès et de rectification des données, ainsi qu'un droit d'opposition au traitement. L'entreprise à l'obligation de veiller à offrir à ses travailleurs la possibilité effective d'exercer ces droits.

5.2.1. Le droit d'accès [62]

Le travailleur a le droit d'obtenir de son employeur, s'il est le responsable du traitement, les renseignements suivants :

- la confirmation que des données le concernant sont ou ne sont pas traitées, les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées ;

---

(60) À l'exception, évidemment, du caractère obligatoire ou non de la réponse ainsi que des conséquences éventuelles d'un défaut de réponse dès lors qu'aucune demande de communication d'informations n'est ici adressée à la personne concernée.

(61) Loi du 8 déc. 1992, art. 9, § 2, d).

(62) Loi du 8 déc. 1992, art. 10.

- la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données ;
- la connaissance de la logique qui sous-tend tout traitement automatisé des données qui le concernent dans les cas des décisions automatisées produisant des effets juridiques à l'égard du travailleur ou l'affectant de manière significative [63] ;
- un avertissement de la faculté d'exercer les recours légaux possibles [64] et de consulter le registre public tenu par la Commission [65].

5.2.1. Le droit de rectification, d'opposition, de suppression et d'interdiction [66]

Toute personne peut obtenir gratuitement la rectification de données inexactes la concernant [67].

Il est en principe également possible à toute personne concernée de s'opposer à ce que des données la concernant fassent l'objet d'un traitement, pour autant qu'elle invoque des motifs légitimes et sérieux tenant à une situation particulière. Un salarié ne pourra toutefois pas s'opposer au traitement de ses données nécessaires à l'exécution de son contrat de travail ou au respect par l'employeur de ses obligations légales ou réglementaires [68].

Toute personne a enfin le droit d'obtenir la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la

---

(63) Il est ici fait référence aux décisions automatisées au sens de l'article 12 *bis* de la loi. Cet article dispose qu'une décision qui produit des effets juridiques à l'égard d'une personne ou qui l'affecte de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité. L'exemple type ici est celui de décisions de promotion, voire de licenciement, qui seraient prises sur la base d'un système d'évaluation automatisé des salariés. Cette interdiction ne s'applique cependant pas si la décision est prise dans le cadre d'un contrat, par exemple un contrat de travail, ou est fondée sur une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance. La disposition ou le contrat doivent toutefois contenir des mesures appropriées, garantissant la sauvegarde des intérêts légitimes du travailleur. Il devra au moins être permis à celui-ci de faire valoir utilement son point de vue.

(64) Tels que prévus aux articles 12 et 14 de la loi du 8 décembre 1992.

(65) Tel que prévu à l'article 18 de la loi du 8 décembre 1992.

(66) Loi du 8 déc. 1992, art. 12.

(67) Art. 12, § 1er, loi du 8 déc. 1992.

(68) Art. 12, § 1er, al. 2, loi du 8 déc. 1992.

concernant qui, compte tenu du but du traitement, est incomplète ou non pertinente ou dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui a été conservée au-delà de la période autorisée [69].

5.3. La mise en place de mesures internes [70]

La loi du 8 décembre 1992 impose la mise en place de différentes mesures destinées à garantir la confidentialité et la sécurité du traitement. L'employeur qui traite les données de son personnel devra ainsi veiller à respecter ces dispositions légales et à prendre les mesures pratiques qui s'imposent.

Il lui faudra notamment prendre des mesures visant à la tenue à jour des données, en veillant à ce que les données incorrectes, incomplètes ou non pertinentes soient rectifiées ou supprimées. Il devra faire en sorte de limiter l'accès de ses préposés aux données qui leur sont nécessaires pour exercer leurs fonctions ou pour les nécessités du service. De même, il devra faire en sorte que ses préposés aient connaissance du contenu de la législation applicable en matière de vie privée.

En cas de traitement automatisé, les programmes utilisés devront être conformes avec les termes de l'éventuelle déclaration à effectuer. Il faudra également s'assurer de la régularité de leur application.

Des mesures concrètes, techniques et organisationnelles, devront également être prises pour empêcher la destruction, la perte et, de manière générale, tout traitement non autorisé comme la modification ou l'accès des données. Ces mesures devront assurer une protection adéquate compte tenu, d'une part, de l'état de la technique et de leur coût et, d'autre part, de la nature des données en cause et des risques. À titre d'exemples, on peut citer la mise en place d'un système d'alarme vol et incendie ou encore la protection du réseau informatique par le biais de firewalls et de procédures d'identification des utilisateurs.

---

(69) Art. 12, § 1er, al. 5, loi du 8 déc. 1992.
(70) Art. 16, loi du 8 déc. 1992.

Si le responsable du traitement confie le traitement à un sous-traitant [71], des mesures supplémentaires s'imposent à lui [72]. Il convient en effet d'éviter une déperdition de sécurité liée au transfert du traitement.

5.4. L'obligation de déclaration

5.4.1. Principes

La mise en place de mesures internes ne suffira pas à assurer le respect du prescrit légal. L'entreprise responsable d'un ou plusieurs traitements partiellement ou entièrement automatisés ayant des finalités semblables ou liées devra préalablement à sa ou à leur mise en œuvre le ou les déclarer à la Commission [73]. Les traitements non automatisés sont exclus du champ d'application de cette disposition [74].

Il semble que la loi ait voulu *"alléger l'obligation de déclaration en permettant d'opérer une même déclaration pour différentes finalités liées à un ou plusieurs traitements"*, les circonstances de fait étant déterminantes pour apprécier le nombre de déclarations à effectuer [75]. Le site de la Commission se réfère à l'hypothèse d'un responsable de traitement disposant de plusieurs établissements sur le territoire belge et désirant déclarer pour ces établissements le même traitement et indique quand, dans ce cas, une seule déclaration doit être effectuée, *"reprenant le nom et l'adresse du siège social ou du siège administratif"* [76].

Ce site reprend également une liste de finalités les classant en différentes catégories au sein desquelles les finalités reprises sont considérées comme liées et ne devront dès lors donner lieu qu'à une seule déclaration [77]. La marche à suivre et les formulaires de déclaration, de même que les tarifs applicables, sont disponibles sur le site de la Commission.

---

(71) On songe, dans le contexte professionnel, aux secrétariats sociaux, aux services de prévention externes, etc.

(72) Pour plus de détails, voir art. 16, § 1er, loi du 8 déc. 1992.

(73) Loi du 8 déc. 1992, art. 17, § 5.

(74) Ils font l'objet d'une autre disposition, l'article 19, qui confère à la Commission le droit d'enjoindre au responsable du traitement de lui communiquer les informations visées par l'obligation de déclaration.

(75) Th. LEONARD, *op. cit.*, p. 49, n° 670.

(76) *http//www.privacy.fgov.be/declarations/lexique1.htm.*

(77) *http/ ::www.privacy.fgov.be/declarations/lexique2.htm.*

Il convient encore de relever que la suppression d'un traitement automatisé de même que toute modification d'une des informations reprises dans la déclaration originelle doit faire l'objet d'une déclaration spécifique [78].

5.4.2. Exemptions

La loi autorise le Roi à établir des exemptions à l'obligation de déclaration, dans les cas où il n'y a manifestement pas de risque d'atteinte aux droits et libertés des personnes concernées, et pour autant que soient précisées les finalités du traitement, les catégories de données traitées, les catégories de personnes concernées, les catégories de destinataires et la durée de conservation des données [79].

Les exemptions plus particulièrement pertinentes dans le contexte professionnel sont exposées ci-dessous :

(i) L'administration par l'entreprise des salaires de ses travailleurs [80]

L'exemption relative à l'administration des rémunérations est subordonnée à la condition que les données soient exclusivement utilisées pour l'administration des rémunérations [81], qu'elles ne soient communiquées qu'aux destinataires "qui en ont droit" et enfin qu'elles ne soient pas conservées au-delà du temps nécessaire [82].

---

(78) Loi du 8 déc. 1992, art. 17, § 7.

(79) Loi du 8 déc. 1992, art. 17, § 8.

(80) A.R. du 13 févr. 2001, art. 51. Il ressort du rapport au Roi que le terme "salaire" au sens de la loi doit être compris de façon très large. Il comprendra dès lors non seulement la rémunération, fixe ou variable, au sens strict mais également tous les avantages acquis en vertu du contrat de travail (titres-repas, voiture de société, assurances groupe...).

(81) Ni la loi ni l'arrêté royal ne définissent quels traitements sont visés par l'expression "administration des salaires". Selon Th. LEONARD, il faut y inclure notamment les opérations de calcul des rémunérations et de cotisations de toute nature donnant lieu à des retenues. Selon nous, il convient également d'y inclure les paiements proprement dits, l'établissement et l'envoi des fiches de rémunération...

(82) Il convient ici de tenir compte, d'une part, de certaines dispositions légales prescrivant, pour certains documents, une durée de conservation précise, comme par exemple celle concernant la conservation des documents sociaux. D'autre part, il semble légitime que l'employeur conserve les données relatives à tel ou tel travailleur dont le contrat de travail a pris fin pendant la durée du délai de prescription – en principe d'un an – afin de pouvoir, le cas échéant, défendre ses intérêts dans le cadre d'un litige éventuel avec le travailleur concerné.

(ii) L'administration par l'entreprise de son personnel [83]

La seconde exemption porte sur les traitements visant exclusivement l'administration du personnel [84] travaillant pour l'entreprise à condition que le traitement ne porte ni sur des données sensibles [85] ni sur des données destinées à une évaluation du travailleur concerné, que les données ne soient pas communiquées à des tiers, sauf dans le cadre de l'application d'une obligation légale ou réglementaire ou pour autant qu'elles soient indispensables à la réalisation des objectifs du traitement et, enfin, qu'elles ne soient pas conservées au-delà du temps nécessaire.

6. Le transfert des données vers des pays situés hors de l'Union européenne [86]

Le transfert de données à caractère personnel concernant le personnel d'une entreprise est soumis aux principes et règles exposés ci-dessus tant que ce transfert s'inscrit dans les limites du territoire national. Il est soumis aux principes édictés par la directive 95/46/CE du 24 octobre 1995 et, le cas échéant, aux législations nationales ayant transposé la directive applicables, lorsqu'il concerne le transfert vers des pays situés au sein de l'Union européenne.

Dans l'un et l'autre cas, ce transfert est en principe autorisé, sous réserve des dispositions et restrictions spécifiques prévues par la directive ou la législation nationale applicable.

6.1. Le principe

Lorsqu'il s'agit du transfert de données personnelles de l'Union européenne vers un pays hors Union européenne, le principe est inversé : le transfert est, en principe, interdit sauf si le pays en question

---

(83) A.R. du 13 févr. 2001, art. 52.

(84) L'administration du personnel n'est pas définie par la loi mais comprend, selon C. DE TERWAGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal", *J.T.*, 2001, p. 463 : la sélection et le recrutement du personnel, la formation, l'organisation du travail, des plans de carrière...

(85) L. du 8 déc. 1992, art. 6, 7 et 8.

(86) La problématique étant vaste et complexe, celle-ci ne sera qu'esquissée dans la présente contribution. Pour une analyse plus approfondie, voir, notamment, B. HAVELANGE et A-Ch. LACOSTE, "Les flux transfrontaliers de données à caractère personnel en droit européen", *J.T. Droit européen*, 2001, p. 241 et suiv.

assure un niveau de protection adéquat et moyennant le respect des dispositions de la loi du 8 décembre 1992 et de ses arrêtés d'exécution [87].

S'il revient en théorie au responsable du traitement d'apprécier ce caractère adéquat, il ne pourra, en pratique, considérer qu'un pays tiers présente un niveau de protection adéquat que pour autant que celui-ci soit inscrit sur une sorte de liste blanche établie par la Commission européenne. Y figurent actuellement les pays suivants : Canada, Argentine, Suisse, Guernesey et l'île de Man. Pour les États-Unis, il existe un régime tout à fait spécifique, dénommé Safe Harbor [88].

En pratique, la nécessité de transférer des données concernant le personnel vers des pays situés hors de l'Union européenne est toutefois fréquente, en particulier dans les groupes multinationaux. Afin d'éviter une impossibilité absolue de transfert hors Union européenne, lorsque le niveau de protection du pays vers lequel le transfert est envisagé n'est pas adéquat, la loi du 8 décembre 1992 propose néanmoins plusieurs possibilités pour néanmoins réaliser un tel transfert.

6.2. Les dérogations

Le transfert de données personnelles relatives aux travailleurs de l'entreprise vers des pays ne présentant pas le niveau de protection sera possible dans les cas suivants :

- lorsque le travailleur a indubitablement donné son consentement au transfert envisagé. Compte tenu de cette exception, il est conseillé, le cas échéant, de prévoir une clause spécifique en ce sens, dans le contrat de travail ;
- lorsque le transfert concerné est nécessaire à l'exécution du contrat de travail ou de mesures préalables à la conclusion de ce contrat, prises à la demande du (candidat) travailleur. Cette exception pourrait, par

---

(87) Loi du 8 déc. 1992, art. 21.

(88) Celui-ci implique, en substance, l'inscription des entreprises vers lesquelles un transfert est autorisé sur une liste des entreprises adhérant aux "Safe Harbour Principles" publiée par le Ministère du Commerce des États-Unis d'Amérique. En réalité, le système mis en place en ce qui concerne ce dernier pays est bien plus complexe. Il ne peut toutefois être examiné dans la cadre du présent article. Le lecteur intéressé se référera utilement, notamment, à l'article de B. HAVELANGE et A-Ch. LACOSTE, "Les flux transfrontaliers de données à caractère personnel en droit européen", *J.T. Droit européen*, 2001, p. 241 et suiv.

exemple, s'appliquer à un contrat de détachement ou encore à l'exécution d'un plan d'options sur actions ;

- lorsque le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt du travailleur, entre l'entreprise et un tiers. Cette exception pourrait, selon nous, s'appliquer à un contrat conclu entre un employeur et un assureur groupe.

De façon plus générale, le manque de protection adéquate pourra encore être résolu par la mise en place d'un mécanisme de garanties suffisantes, celles-ci pouvant être de nature technique et/ou contractuelle. Il s'agira, par exemple, de démontrer que la protection adéquate est assurée par l'existence, au sein du groupe concerné, d'un *Business Conduct Code* ou règlement analogue présentant des garanties similaires à celles prévues par la loi. La procédure est toutefois quelque peu fastidieuse dans la mesure où elle implique une autorisation accordée par arrêté royal...[89].

Une dernière possibilité est offerte par la Commission européenne elle-même qui publie périodiquement des exemples de clauses fournissant un niveau de protection adéquat. Le 7 janvier 2005, la Commission a d'ailleurs approuvé de nouvelles clauses type [90].

(89) Loi du 8 déc. 1992, art. 22.

(90) Elles peuvent être consultées sur le site de l'Union européenne.

7. Les sanctions [91]

7.1. Les sanctions pénales [92]

Les articles 37 et suivants de la loi du 8 décembre 1992 prévoient les sanctions pénales applicables en cas de violation de la loi. Les peines prévues à titre principal consistent en des amendes. L'emprisonnement est possible dans certaines hypothèses, notamment en cas de récidive [93]. L'entreprise, considérée comme le responsable du traitement, ou son représentant en Belgique, est civilement responsable du paiement des amendes auxquelles son préposé ou mandataire est condamné.

À notre connaissance, aucune condamnation pénale du chef d'infraction à la loi du 8 décembre 1992 n'a encore été prononcée en Belgique. En France, en revanche, la cour d'appel de Versailles a condamné, par arrêt du 3 mars 2003, deux employés du service des ressources humaines d'une entreprise en raison d'un détournement de la finalité d'un traitement automatisé [94].

---

(91) Nous n'examinerons pas, dans le cadre de cette contribution, les compétences de contrôle étendues et variées dont dispose la Commission ni les procédures judiciaires particulières susceptibles d'être mises en œuvre afin d'assurer le respect de la loi. Pour plus de détails, voir E. PLASSCHAERT et J.-A DELCORDE, "Le traitement et la protection des données personnelles des travailleurs, *Or.*, Numéro spécial contenant les actes du colloque du 10 mars 2005 relatif à l'employeur et la vie privée au travail.

(92) L. du 8 déc. 1992, art. 37 et suiv.

(93) La loi prévoit également des peines adaptées à la matière : le juge peut ainsi tantôt ordonner la publication du jugement dans un ou plusieurs journaux, tantôt ordonner la confiscation des supports matériels des données à caractère personnel (à l'exclusion des ordinateurs), ou encore ordonner l'effacement de ces données. Il peut enfin, dans certains cas, interdire au condamné de gérer tout traitement de données à caractère personnel, pendant une durée de deux ans maximum.

(94) Arrêt cité sur le site web de la CNIL, *www.cnil.fr.*

7.2. Les sanctions civiles

7.2.1. Les sanctions civiles directes

Nous entendons ici par sanction civile directe l'action en responsabilité de droit commun à laquelle s'expose l'entreprise qui causerait à autrui un dommage en relation causale avec la violation d'une ou plusieurs dispositions de la loi du 8 décembre 1992 [95].

7.2.2. Les sanctions civiles indirectes

Nous entendons par sanction civile indirecte la sanction qui découle pour l'entreprise de l'inopposabilité à la personne concernée des éléments de preuve relatifs à quelque manquement contractuel ou extracontractuel, voire à une infraction pénale, lorsque ceux-ci ont été recueillis en violation des dispositions de la loi du 8 décembre 1992.

Cette problématique étant par ailleurs largement examinée par d'autres dans le présent ouvrage, notamment suite au récent arrêt du 2 mars 2005, nous ne nous y attarderons pas si ce n'est pour souligner qu'en dehors du contentieux en matière de licenciement pour motif grave impliquant la question de la légitimité des éléments de preuves recueillis par le biais de caméras de surveillance ou à l'occasion du contrôle des courriels, de l'accès à Internet ou de l'analyse du disque dur, il existe à ce jour peu, voire pas, de jurisprudence en la matière concernant d'autres types de traitements.

En France, la Cour de cassation a eu à connaître d'une affaire impliquant le non-respect des dispositions en matière de protection des données lors de la mise en œuvre d'un dispositif automatisé des entrées et sorties des salariés au moyen de badges. Elle a rejeté le pourvoi formé contre un arrêt qui avait décidé que le licenciement d'un travailleur qui avait refusé, à de nombreuses reprises, d'utiliser son badge d'entreprise à la sortie de l'entreprise était sans cause réelle et sérieuse en raison du défaut de déclaration du traitement à la CNIL [96].

---

(95) Signalons une particularité. L'article 15 *bis* de la loi prévoit que lorsque une violation de celle-ci cause un dommage à la personne concernée, le responsable du traitement en sera responsable à moins de prouver que le fait générateur ne lui est pas imputable. Il s'agit donc d'une présomption réfragable de responsabilité. Celle-ci s'applique sans préjudice d'actions fondées sur d'autres dispositions légales.

(96) Cass. fr., 6 avr. 2004, *www.courdecassation.fr.*

C. LE CONTRÔLE PAR L'EMPLOYEUR DES PRESTATIONS DE TRAVAIL OU LES NOUVELLES POSSIBILITÉS DE CONTRÔLE SPATIO-TEMPOREL

1. Observations liminaires

De tous temps l'employeur a eu la volonté de contrôler les prestations de travail de ses salariés en étant, notamment, en mesure de localiser ceux-ci et d'enregistrer leur temps de travail. Les nouvelles technologies, permettant désormais un contrôle bien plus étendu, précis et performant, ont considérablement contribué à augmenter le risque d'une immixtion excessive de l'entreprise dans la sphère privée du travailleur. La probabilité d'atteinte à la part irréductible de vie personnelle qui doit rester garantie, même au temps et lieu de travail, est ainsi devenue beaucoup plus tangible.

De nouvelles règles spécifiques, que celles-ci trouvent leur source dans la loi, dans les dispositions réglementaires ou contractuelles ou dans les codes de bonne conduite, dans les usages, dans de nouvelles pratiques..., sont alors nées afin de mieux encadrer la mise en œuvre des nouveaux dispositifs de contrôle du temps de travail et, surtout, de géolocalisation des travailleurs. Nous examinerons ci-après la question de la protection des données recueillies et traitées dans le cadre du contrôle du temps de travail et de la géolocalisation de travailleurs [97].

2. La localisation des travailleurs

Associant les technologies GPS et GSM, il existe désormais des systèmes permettant à l'employeur de suivre, le cas échéant en temps réel, le déplacement de ses salariés dont les fonctions impliquent des prestations à l'extérieur (représentants de commerce, consultants, chauffeurs de taxis ou de véhicules de dépannage...).

Le schéma est le suivant : une demande d'information est adressée par le biais du réseau GSM. Le récepteur GPS à bord du véhicule calcule en temps réel la position de ce dernier et renvoie l'information par le réseau GSM central, qui affiche la situation sur une carte routière [98].

---

(97) Nous n'examinerons pas les dispositions spécifiques régissant tel ou tel système de contrôle des prestations de travail particulier, comme la vidéosurveillance, susceptibles de s'appliquer concurremment.

(98) Les services de géolocalisation GSM/GPS, *www.cnil.fr*.

Les informations ainsi disponibles peuvent concerner le trajet effectué, les temps d'arrêt, les heures de départ et d'arrivée, voire la vitesse des véhicules. Dans la mesure où ces informations peuvent être rattachées à une personne, elles doivent être considérées comme des données à caractère personnel.

2.1. Les enjeux de la géolocalisation au regard de la protection de la vie privée

Dès lors que des données de géolocalisation sont des données à caractère personnel, toutes les conditions générales auxquelles la loi subordonne tout traitement, telles qu'exposées ci-dessus, doivent être remplies. Nous nous bornerons ici à préciser les questions spécifiques que soulève ce type de traitement et à esquisser des réponses possibles [99].

Le traitement de telles données présente des risques certains au regard des libertés et droits fondamentaux du travailleur dès lors que celui-ci peut être suivi dans tous ses déplacements. Comme l'expose la CNIL, la géolocalisation soulève dès lors principalement deux questions : celle de la frontière entre travail et vie privée et celle du niveau de contrôle permanent qu'il est admissible de faire peser sur un travailleur [100].

La première question doit être résolue par l'adoption de modalités de mise en œuvre des dispositifs de géolocalisation qui soient respectueuses de la sphère privée des travailleurs (possibilité de désactivation du dispositif pendant les temps de repos, durée de conservation des données, condition d'accès et de sécurité...). Il s'agira ici d'une application du principe du traitement adéquat, pertinent et non excessif des données.

La réponse à la deuxième question sera d'abord fonction de la finalité du traitement. Le principe de proportionnalité permettra ensuite de déterminer le niveau de contrôle permanent qu'il est admissible de faire peser sur un travailleur. Ainsi il est évident que le traitement de données de géolocalisation par des entreprises de taxis ou de dépannage, où la localisation précise en temps réel de tous les véhicules est de nature

---

(99) Pour plus de détails, voir O. RIJCKAERT, "Surveillance des travailleurs : nouveaux procédés et multiples contraintes, *Or.*, Numéro spécial contenant les actes du colloque du 10 mars 2005 relatif à l'employeur et la vie privée au travail.

(100) La géolocalisation des véhicules mis à disposition des employés : la CNIL prépare une recommandation, *www.cnil.fr*.

à permettre une allocation optimale des ressources disponibles, est de nature à justifier un contrôle plus intense que lorsqu'il s'agit, par exemple, de vérifier la bonne exécution par des représentants de commerce de leur plan de route.

2.2. De quelques conditions du traitement de données de géolocalisation

Les dispositifs de localisation des travailleurs suscitent des interrogations spécifiques quant à la nécessité d'obtenir le consentement du travailleur concerné et de déclarer un tel traitement à la Commission préalablement à sa mise en œuvre.

2.2.1. Le travailleur concerné doit-il donner son consentement ?

Sauf à considérer qu'un tel traitement est nécessaire à l'exécution du contrat de travail [101], celui-ci ne pourra être mis en œuvre que moyennant le consentement indubitable des travailleurs concernés. Celui-ci peut en principe être implicite dès lors que la loi du 8 décembre 1992 n'exige pas que celui-ci soit donné par écrit, sauf traitement de données sensibles. L'employeur devra toutefois être en mesure de démontrer que ce consentement fut libre, spécifique et que le travailleur concerné l'a donné en pleine connaissance de cause.

La récente loi du 13 juin 2005 relative aux communications électroniques dispose, en outre, que les opérateurs de réseaux mobiles qui traitent des données de localisation se rapportant à un abonné ou un utilisateur final dans le cadre de la fourniture d'un service de

---

(101) O. RIJCKAERT in "Surveillance des travailleurs : nouveaux procédés et multiples contraintes, *Or.*, Numéro spécial contenant les actes du colloque du 10 mars 2005 relatif à l'employeur et la vie privée au travail, estime que le traitement de telles données de géolocalisation ne peut être considéré comme nécessaire à l'exécution du contrat de travail. Celles-ci, écrit-il, ne sont en rien indispensables à l'exécution du travail en tant que tel. Nous serions enclins à interpréter la notion de nécessité liée à l'exécution du contrat, telle qu'elle figure à l'article 5, b) de la loi du 8 décembre 1992, de façon moins stricte et estimons que de tels dispositifs peuvent, en certaines circonstances, se justifier par référence aux nécessités d'exécution du contrat de travail, par exemple lorsque le dispositif permet à l'employeur de mieux exécuter son obligation de fournir le travail convenu.

localisation doivent préalablement obtenir le consentement, révocable *ad nutum*, de l'abonné ou, le cas échéant, de l'utilisateur final [102].

L'abonné pouvant, en l'espèce, être l'employeur et, l'utilisateur final étant alors le travailleur, la question se pose de savoir comment interpréter la notion "le cas échéant" afin de déterminer s'il s'agit de l'entreprise ou du travailleur concerné qui doit donner son consentement [103]. Il semblerait cohérent de considérer qu'il s'agit du travailleur auquel se rapportent les données qui doit donner son consentement. Si cette interprétation devait se confirmer, elle impliquerait qu'un dispositif de géolocalisation ne pourrait désormais plus être mis en œuvre qu'à condition que les travailleurs concernés aient marqué leur accord, étant entendu qu'ils pourraient à tout moment retirer, définitivement ou temporairement, celui-ci [104].

2.2.2. L'obligation de déclaration du traitement

Enfin, la question de savoir si un tel traitement est un traitement concernant l'administration du personnel bénéficiant d'une exemption de déclaration à la Commission n'est pas évidente. Nous serions enclins de penser que la réponse à cette question n'est pas univoque mais dépendra de la finalité poursuivie.

Si celle-ci est notamment liée à l'organisation du travail [105], il pourrait être soutenu que le traitement bénéficie de l'exemption. La réponse sera sans doute fonction de l'interprétation plus ou moins large de la notion administration du personnel.

Rappelons toutefois que l'exemption prévue en la matière à l'article 52 de l'arrêté royal du 13 février 2001 est fondée sur l'article 17, § 8, de la loi du 8 décembre 1992, qui prévoit la possibilité pour le Roi de prévoir des exemptions lorsque, compte tenu des données traitées, il n'y a manifestement pas de risque d'atteinte aux droits et libertés des personnes concernées. Il n'est pas certain, dès lors, qu'un dispositif de géolocalisation puisse être considéré comme un traitement

---

(102) Loi du 13 juin 2005, art. 123, § 2.

(103) Dans son avis n° 8/2004 du 14 juin 2004 relatif à l'avant-projet de loi relatif aux communications électroniques, la Commission avait déjà souligné cette difficulté d'interprétation.

(104) Loi du 13 juin 2005, art. 123, § 2, 4°.

(105) Considèrent que l'organisation du travail relève de l'administration du personnel : C. DE TERWAGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal" , *J.T.*, 2001, p. 463.

lié à l'administration du personnel [106] ne présentant manifestement pas de risque d'atteinte aux droits et libertés des personnes concernées.

2.3. Considérations finales

Il appartiendra, à l'avenir, à la Commission de contribuer à dessiner les contours de ce qui est possible et de ce qui ne peut être admis en matière de géolocalisation. En deuxième ligne, il reviendra aux cours et tribunaux de tracer les limites. Enfin, il ne peut être exclu que le législateur intervienne également dans le débat [107].

La Commission s'est, incidemment, prononcée sur la question dans son avis n° 8/2004 du 14 juin 2004 relatif à l'avant-projet de loi relatif aux communications électroniques.

La jurisprudence en la matière est, à notre connaissance, quasi inexistante. La seule décision qui nous est à ce jour connue est un arrêt de la cour du travail de Bruxelles du 18 novembre 2004. Saisie d'une demande en autorisation de licenciement pour motif grave d'un chauffeur de taxi [108] s'étant rendu coupable de constants et importants excès de vitesse, constatés grâce à un dispositif de géolocalisation, la cour a admis que la preuve des excès de vitesse invoquée par l'employeur soit rapportée par la production des données recueillies grâce au système GPS.

La régularité des éléments de preuve ainsi recueillis semble ne pas avoir été examinée à la lumière des dispositions de la loi du 8 décembre 1992. Peut-être la solution retenue par la cour aurait-elle alors été différente ? [109]

---

(106) O. RIJCKAERT, "Surveillance des travailleurs : nouveaux procédés et multiples contraintes, *Or.*, Numéro spécial contenant les actes du colloque du 10 mars 2005 relatif à l'employeur et la vie privée au travail, est réticent à admettre que pareil traitement relève de l'administration du personnel.

(107) Le 18 février 2005 a été déposée une proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992, 2004-2005, 3-1044/1, *www.senat.be.* L'objet de celle-ci est toutefois assez limité puisqu'il vise uniquement à subordonner la mise en œuvre d'un tel dispositif à l'accord des commissions paritaires "*ad hoc*", du comité commun à l'ensemble des services publics, ou des organes compétents en vertu du régime des relations de travail (*sic*).

(108) Celui-ci était délégué du personnel suppléant au sein du conseil d'entreprise.

(109) Si la finalité déclarée avait été la gestion de la flotte de véhicules, il est certain que l'utilisation du dispositif en vue d'identifier les excès de vitesse du chauffeur concerné aurait constitué un traitement ultérieur incompatible avec la finalité originelle et, partant,

3. Les systèmes d'enregistrement des accès et du temps de travail

Comme les dispositifs de géolocalisation, les divers systèmes visant à contrôler l'accès à l'entreprise et à enregistrer le temps de travail (cartes d'accès magnétiques ou à puce, frappe d'un code d'accès...) doivent respecter les principes et conditions de mise en œuvre définies par la loi du 8 décembre 1992. Ces systèmes ne sont, contrairement aux dispositifs de géolocalisation, pas nouveaux.

En règle, on peut considérer qu'ils ne sont pas subordonnés au consentement du travailleur et ne doivent pas être déclarés à la Commission [110]. Pour le surplus, ils ne posent généralement pas problème à l'égard de la loi du 8 décembre 1992. Lorsqu'une question surgit, elle concerne souvent l'application concrète du principe de proportionnalité au système envisagé, compte tenu de la portée de celui-ci et de ses implications en ce qui concerne la vie privée du travailleur.

Ainsi, la Commission a estimé que le badge confié par l'entreprise au travailleur pour surveiller ses déplacements ne devait pas mentionner les nom et prénom du travailleur, mais uniquement sa photo et un numéro d'identification [111]. En France, la CNIL a estimé que les traitements concernés ne doivent concerner que les entrées et sorties du lieu de travail et pas permettre le contrôle des déplacements à l'intérieur du lieu de travail, à l'exception des cas dans lesquels certaines zones identifiées font l'objet d'une restriction de circulation justifiée par la sécurité des biens et des personnes qui y travaillent [112].

Les nouvelles technologies, par les nouveaux types de traitements qu'elles ont permis de mettre en œuvre, ont néanmoins suscité de nouvelles questions, notamment quant aux techniques admissibles. En France, le Tribunal de grande instance de Paris a ainsi interdit, par son jugement du 19 avril 2005, la mise en place d'un système de contrôle biométrique utilisant l'empreinte digitale des salariés bagagistes

---

une violation de la loi du 8 décembre 1992. Se serait alors posée la question de l'admissibilité des éléments de preuve recueillis...

(110) En ce sens également, voir O. RIJCKAERT, "Surveillance des travailleurs : nouveaux procédés et multiples contraintes, *Or.*, Numéro spécial contenant les actes du colloque du 10 mars 2005 relatif à l'employeur et la vie privée au travail, p. 59.

(111) Avis n° 2/2004 du 26 févr. 2004, *http://www.privacy.fgov.be.*

(112) Décision reprise sur le site web de la CNIL, *www.cnil.fr.*

chargés de prestations d'accueil et d'accompagnement dans les gares ferroviaires. Ce système était destiné à contrôler les horaires de travail.

Le tribunal a estimé qu'une telle technique, qui met en cause le corps humain et porte ainsi atteinte aux libertés individuelles, n'est pas justifiée lorsqu'elle est utilisée aux seules fins de contrôle des horaires. Le tribunal laisse toutefois entendre qu'elle pourrait l'être lorsqu'elle a une finalité sécuritaire ou protectrice de l'activité exercée dans des locaux identifiés [113].

Signalons enfin que, dans la mesure où de tels traitements visent à mesurer le temps de travail, ils doivent également être mentionnés dans le règlement de travail en application de l'article 6, § 1, 2°, de la loi du 8 avril 1965 instituant les règlements de travail.

D. CONCLUSIONS

La loi du 8 décembre 1992, telle que modifiée par la loi du 11 décembre 1998 transposant la directive n° 95/46/CE du 24 octobre 1995, atteint, dans l'ensemble, son objectif qui est celui de garantir les libertés et droits fondamentaux de tout individu, notamment la protection de sa vie privée. Le régime juridique qu'elle met en œuvre afin de protéger toute personne contre un traitement illégitime de ses données personnelles nous semble adéquat.

Nous nous posons toutefois la question de savoir si cette législation n'est pas, de par son caractère très général, mal ou insuffisamment adaptée au contexte professionnel [114].

L'examen des décisions de jurisprudence, notamment rendues à l'occasion du contentieux du licenciement pour motif grave, que ce soit par des juridictions civiles ou pénales, illustre au demeurant une tendance des cours et tribunaux à pallier les difficultés les plus

---

(113) Délibération n° 02-001 du 8 janvier 2002 concernant les traitements automatisés d'informations nominatives mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration, *www.cnil.fr*.

(114) Dans son avis du 13 septembre 2001 sur le traitement des données à caractère personnel dans le contexte professionnel, le groupe de travail "Article 29" estimait à cet égard qu'*"une orientation sera la bienvenue pour clarifier certains aspects de l'application des dispositions de la directive 95/46/CE dans le contexte professionnel"*. Entre-temps la Commission européenne a déjà procédé à deux phases de consultations des partenaires sociaux en ce qui concerne la protection des données personnelles des travailleurs.

importantes qu'une application trop stricte de la loi du 8 décembre 1992 dans le contexte professionnel pourrait impliquer.

Il en est particulièrement ainsi lorsqu'un travailleur, à l'égard duquel existent des présomptions légitimes d'implication dans des infractions commises au préjudice de l'entreprise, conteste *a posteriori* la régularité des preuves obtenues en violation des dispositions applicables, notamment en violation de la loi du 8 décembre 1992, sous prétexte que l'entreprise n'a pas respecté, lors de la mise en œuvre du traitement ayant permis de confondre le travailleur, les règles prévues par la loi (information de la personne concernée, déclaration du traitement à la Commission...).

Or, dans ce genre de cas, le non-respect de ces règles ne résulte nullement de la volonté de l'entreprise de contourner les dispositions protectrices prévues par la loi mais de l'impossibilité pratique (mise en œuvre trop contraignante ou fastidieuse pour un cas isolé, risque d'éveiller les soupçons de l'intéressé, etc.) d'appliquer les règles strictes et, dans de tels cas trop rigides, prévues.

Dès lors, nous semble-t-il, se pose la question de l'opportunité d'une adaptation de la loi afin de permettre, dans des circonstances exceptionnelles et moyennant un contrôle judiciaire *a posteriori*, de déroger aux conditions habituelles de licéité applicables aux traitements de données à caractère personnel.

Déjà dans son recueil de directives [115], le Bureau international du travail avait admis que le contrôle pouvait être secret lorsqu'il y avait des soupçons raisonnables quant à l'implication d'un travailleur dans une infraction pénale ou quant à un manquement grave. La jurisprudence semble désormais également de plus en plus encline, dans des cas impliquant une infraction pénale, soit à interpréter de façon restrictive le champ d'application des dispositions protectrices de la vie privée [116], soit à admettre la régularité des preuves obtenues lorsque "l'illicéité commise est sans commune mesure avec la gravité de l'infraction dont l'acte irrégulier a permis la constatation, ou que cette irrégularité est sans incidence sur le droit ou la liberté protégés par la

---

(115) "Protection des données personnelles des travailleurs», *Recueil de directives pratiques du BIT*, articles 6.14 (2) (a) et (b).

(116) La Cour de cassation française a ainsi admis qu'un risque ou évènement particulier pouvait justifier qu'un employeur ouvre les fichiers identifiés comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition par l'entreprise (Cass. fr., 17 mai 2005, arrêt cité sur le site de la CNIL, *www.cnil.fr*).

norme transgressée" [117]. Enfin, la loi du 8 décembre 1992 fait-elle même référence, à au moins une occasion, à la *"prévention d'un danger concret ou la répression d'une infraction pénale"* afin de justifier une dérogation aux règles de traitement normalement applicables [118].

Dans ces conditions, ne serait-il pas opportun, plutôt que de voir les cours et tribunaux contraints de justifier *a posteriori*, dans des cas exceptionnels, un traitement opéré en violation des règles normalement applicables, que le législateur intervienne en prévoyant, une dérogation générale à ces principes dans des cas exceptionnels, le juge n'intervenant plus qu'en vue de vérifier le caractère exceptionnel du cas en question ?

* * *

(117) Cass., 2 mars 2005, P.04.1644.F/5, *www.juridat.be.*
(118) Loi du 8 déc., 1992, art. 7, § 4.