Gestion et protection des données à caractère personnel dans la relation de travail

Rosier, Karen

Published in:
Le droit du travail à l'ère du numérique

Publication date:
2011

Document Version
le PDF de l'éditeur

Gestion et protection des données à caractère personnel dans la relation de travail

Karen Rosier

Avocate au barreau de Namur
Chercheuse au Centre de Recherche Information, Droit et Société (CRIDS) – F.U.N.D.P.
Assistante à la faculté de droit des F.U.N.D.P.

Introduction[1]

1. La législation en matière de protection des données devenue incontournable

1. L'informatisation des entreprises et des administrations a entraîné une révolution dans la gestion des informations. Il est indéniable qu'actuellement, la plupart des entreprises gèrent les données dont elles ont besoin pour leur fonctionnement grâce à l'outil informatique. Qu'il s'agisse d'enregistrer des données, de les rechercher, de les communiquer, l'ordinateur et l'internet sont devenus incontournables. Ceci inclut également la gestion des données relatives aux membres du personnel. L'une des conséquences de cette évolution est que l'application de la loi sur les données à caractère personnel est elle aussi devenue incontournable[2].

2. Tant dans le cadre du processus de recrutement, qu'au cours de l'exécution du contrat ou même lorsque le contrat a pris fin, l'employeur est tenu de respecter certaines règles lorsqu'il traite des données à caractère personnel relatives à des travailleurs. En effet, la loi du 8 décembre 1992 relative à la protec-

---

1 L'auteur tient à remercier chaleureusement le Professeur Cécile de Terwangne pour ses judicieuses suggestions.

2 Pour une autre contribution consacrée à la question du traitement des données à caractère personnel dans le contexte de la relation de travail, voyez E. Plasschaert et J.-A. Delcorde, « Le traitement des données personnelles des travailleurs », *Orientations*, n° spécial 35 ans, mars 2005, pp. 26 et s.

tion de la vie privée à l'égard des traitements de données à caractère personnel[3] et son arrêté royal d'exécution du 13 février 2001[4] qui déterminent certaines conditions et limites au traitement de données sont entièrement applicables au secteur professionnel.

2. La protection de données plus que de la vie privée

3. La législation relative à la protection des données ne date pas d'hier. La loi relative à la protection de la vie privée à l'égard du traitement des données à caractère personnel a été adoptée le 8 décembre 1992[5]. Elle a été profondément remaniée par la loi du 11 décembre 1998 pour transposer la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[6-7]. Cette directive poursuit un double objectif: celui de permettre la libre circulation des données à caractère personnel entre États membres et au sein des États membres, d'une part, et celui de préserver un niveau de protection de la vie privée des personnes physiques satisfaisant, en conformité avec les exigences de l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, d'autre part.

4. La protection qu'offre la législation relative au traitement de données à caractère personnel va cependant au-delà de la protection de la sphère privée. En effet, cette législation entend protéger, dans certains traitements, toute donnée dès lors qu'elle a trait à une personne physique identifiée ou identifiable. De ce fait, sont également concernées les données relatives au milieu professionnel.

5. Par ailleurs, il y a lieu d'éviter la confusion, fréquemment faite, entre protection des données à caractère personnel et obligation de confidentialité. La législation sur la protection des données, inspirée par la directive 95/46/

---

3 *M.B.*, 18 mars 1993.

4 *M.B.*, 13 mars 2001.

5 Et s'inspirait des travaux du Conseil de l'Europe qui avaient déjà dessiné les contours de cette législation dans la Convention nº 108 pour la protection des données (Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, STE Nº 108, le 28 janvier 1981, entrée en vigueur le 1er octobre 1985).

6 *M.B.*, 3 février 1999. La loi du 11 décembre 1998 transpose la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données. Les modifications apportées par la loi du 11 décembre 2008 à la loi du 8 décembre 1992 ne sont cependant entrées en vigueur qu'en 2001. L'entrée en vigueur était en effet subordonnée à l'adoption de mesures d'exécution dans un arrêté royal qui ne fut promulgué que le 13 février 2001.

7 Le droit à la protection des données à caractère personnel est désormais explicitement consacré à l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

CE a pour objet d'autoriser le traitement de données à caractère personnel moyennant le respect de certaines conditions. La confidentialité vise à restreindre l'usage de données en en interdisant la communication à des tiers. Si la législation relative à la protection des données soumet la communication de données à caractère personnel à certaines conditions (dont, dans certains cas, une obligation d'en assurer la confidentialité), elle ne se réduit pas à une problématique de confidentialité.

3. Une législation difficile à appliquer ? Quelques repères…

6. Afin d'assurer un équilibre entre la protection des données à caractère personnel et la nécessité de pouvoir traiter ces données dans le cadre de la vie économique et sociale, la législation adoptée repose essentiellement sur des principes impliquant une pondération des intérêts en présence au cas par cas. Cette approche présente l'avantage d'une régulation suffisamment abstraite que pour pouvoir s'appliquer à tous les secteurs d'activités et à tous les cas de figure. Elle fait toutefois peser sur les personnes censées l'appliquer le devoir et le risque de l'application concrète des dispositions de la loi.

7. Ceci étant, il existe une certaine logique dans la loi qui s'articule essentiellement autour de trois principes : finalité, proportionnalité et transparence. Le principe de finalité implique que l'utilisation de données à caractère personnel ne puisse être faite que pour des finalités, précises et déterminées à l'avance. Le second principe, de proportionnalité, est directement en lien avec le premier puisqu'en découle l'exigence d'une légitimité dans la finalité d'utilisation. Ce principe impose également l'obligation de ne traiter que les données qui sont nécessaires et pertinentes pour réaliser la finalité déterminée et de supprimer les données dès qu'elles ne sont plus nécessaires. Pour assurer la transparence du traitement, la personne qui traite les données devra fournir certaines informations aux personnes concernées[8] et faire une déclaration de traitement auprès la Commission de la protection de la vie privée[9]. Parmi ces informations, figurent la ou les finalités d'utilisation des données.

8. De plus, il a été instauré dans chaque État de l'Union européenne une autorité de contrôle chargée de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de la directive européenne[10]. En Belgique, il s'agit de la Commission de la protection de la vie privée qui émet des avis et des recommandations sur des problématiques

---

8 Art. 9 de la loi du 8 décembre 1992.

9 Art. 17 de la loi du 8 décembre 1992. Il existe cependant des exceptions à ces obligations, définies par l'arrêté royal d'exécution du 13 février 2001 (art. 51 et s. de l'A.R. du 13 février 2001).

10 Art. 28 de la Directive 95/46/CE.

particulières posées par l'application de cette loi. Ces avis et recommandations sont librement consultables sur le site internet de la Commission[11]. Il peut donc être fait appel à cette Commission pour obtenir des précisions et explications en cas de doute sur l'application de la loi. On soulignera encore qu'un travail de réflexion sur la manière d'appliquer la législation de la protection des données est également mené au niveau européen, notamment par le biais du groupe dit de l'Article 29. Ce groupe, qui tient son nom du fait qu'il a été institué par l'article 29 de la directive 95/46/CE, est un organe consultatif européen, composé en autres de représentants de chaque autorité de contrôle des États membres et qui rend des avis publiés sur un site internet[12]. Les avis et autres documents de travail du Groupe de l'Article 29 et de la Commission de la protection de la vie privée n'ont pas de force contraignante mais peuvent être utiles à l'interprétation de la législation sur la protection des données.

4. Objet de notre propos

9. La présente contribution se concentrera sur les implications que peut avoir la législation relative à la protection des données dans le cadre de la relation de travail. Étant donné les problématiques nombreuses et variées qui peuvent graviter autour de ce thème, nous nous concentrerons plus particulièrement sur le traitement mis en œuvre par l'employeur, portant sur des données relatives aux travailleurs et sur la participation du travailleur aux traitements mis en œuvre dans l'entreprise. Il reste toutefois qu'il existe ça et là, au sein de législations distinctes de la loi du 8 décembre 1992 et des arrêtés d'exécution, de nombreuses lois et réglementations qui contiennent des dispositions portant directement ou indirectement sur la protection des données, notamment dans le secteur des relations de travail[13]. Nous ne pourrons toutes les évoquer.

10. La première partie de cette contribution se propose d'aborder la loi sous un angle pragmatique, en définissant pas à pas les questions à se poser dès avant la mise en œuvre d'un traitement de données. Nous nous éloignerons donc de la structure de la loi pour privilégier une présentation des problématiques dans l'ordre où elles peuvent logiquement se poser lorsque l'employeur envisage un traitement de données.

Dans un premier temps, nous nous emploierons à exposer les critères retenus par la loi pour son application matérielle et territoriale ce qui nous permettra de répondre à la question de savoir si la loi du 8 décembre 1992

---

11 www.privacycommission.be.

12 http://ec.europa.eu/justice/policies/privacy.

13 Voy. notamment les C.C.T. n° 68, 81 et 100 et la loi du 28 janvier 2003 relative aux examens médicaux dans le cadre des relations de travail.

s'applique ou non à des opérations concrètement envisagées dans le cadre d'un traitement de données. Nous nous pencherons ensuite sur les dispositions légales qui pourraient empêcher, dans son principe même, la mise en œuvre d'un traitement. Si l'esprit de la loi est d'autoriser le traitement de données à caractère personnel moyennant le respect de certains principes et conditions, tout traitement n'est toutefois pas permis. Cette seconde section nous permettra donc de déterminer si le traitement, tel qu'envisagé, ne contrevient pas à une disposition de la loi. Dans une troisième section, nous nous attacherons à passer en revue les conditions et principes posés par la loi pour la mise en œuvre du traitement. Il s'agira donc de façonner un traitement de données pour en assurer la conformité par rapport aux exigences légales. La dernière section sera consacrée aux droits des personnes concernées par le traitement. L'employeur qui met en œuvre un traitement de données doit être en mesure d'assurer un exercice effectif des droits des travailleurs concernés.

La seconde partie de notre contribution évoquera succinctement la problématique du respect de la loi du 8 décembre 1992 sous un autre angle : celui du rôle et des responsabilités du travailleur qui, dans le cadre de ses prestations, met en œuvre le traitement de données réalisé par son employeur.

Chapitre 1
Le travailleur sujet du traitement de données

Étape 1
Vérifier si la loi sur la protection des données s'applique

11. Dès lors que l'employeur a l'intention de faire usage de données portant sur un ou plusieurs travailleurs, il convient de se poser la question de l'application de la loi du 8 décembre 1992. Cette loi ne prévoit pas de système pour remédier à une irrégularité et rendre le traitement légal si toutes les conditions posées par elle pour le traitement de données à caractère personnel n'ont pas été respectées dès le début de ce traitement ; d'où l'importance de considérer ces questions de protection des données à caractère personnel dès avant la mise en œuvre d'un traitement.

12. La loi du 8 décembre 1992 consacre le principe de responsabilité civile du responsable de traitement en cas de non-respect de ses dispositions. Ainsi, lorsque la personne concernée subit un dommage causé par un acte contraire

aux dispositions déterminées par ou en vertu de la loi du 8 décembre 1992, le responsable du traitement est tenu de réparer le dommage qui en a résulté dans le chef de cette personne. Il est toutefois exonéré de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable[14]. Il n'est pas inutile de pointer, par ailleurs, que le non-respect de la plupart des dispositions de la loi du 8 décembre 1992 est sanctionné pénalement.

Au regard de ce qui précède, on comprend que la gestion des données des travailleurs par l'employeur implique la prise en compte de la loi du 8 décembre 1992.

13. Afin de se conformer à celle-ci, il nous semble nécessaire de se poser, dès avant la mise en œuvre d'un traitement, les bonnes questions. La première est de vérifier si la loi du 8 décembre 1992 s'applique, ce qui implique qu'il y ait un traitement de données à caractère personnel mis en œuvre par un responsable de traitement agissant dans le cadre d'un établissement situé sur le territoire belge ou établi hors de l'Union européenne mais utilisant des moyens localisés sur le territoire belge.

Section 1
A-t-on affaire à un traitement de données à caractère personnel ?

14. La loi du 8 décembre 1992 s'applique à tout traitement totalement ou partiellement automatisé (par des moyens électroniques) et aux traitements manuels (travail sur des fichiers papier ou microfiches)[15] dès que, dans ce dernier cas, les données à caractère personnel sont contenues ou appelées à figurer dans un fichier.

A. Quelques notions clés

1. Qu'entend-on par « donnée à caractère personnel » ?

15. Une donnée à caractère personnel est toute information qui concerne une personne physique identifiée ou identifiable (que l'on appellera la « personne concernée »)[16].

L'*information* peut être de toute nature : il peut s'agir d'un nom, d'une photographie, d'une image vidéo, d'une empreinte digitale, d'un cliché d'ADN,

14 Art. 15*bis* de la loi du 8 décembre 1992.
15 Art. 3 de la loi du 8 décembre 1992.
16 Art. 1, § 1er de la loi du 8 décembre 1992.

d'un numéro de compte en banque, d'un enregistrement vocal, etc. Par ailleurs, il peut s'agir tant d'informations objectives telles que le nom ou la situation familiale d'une personne que de données subjectives tels des avis ou appréciations se rapportant à cette personne[17].

> Le Groupe de l'Article 29 a ainsi précisé à cet égard que :
>
> « Le champ d'application de cette définition implique que la notion de donnée personnelle peut inclure non seulement les données administratives ou qui résultent de facteurs objectifs pouvant être vérifiés ou rectifiés, mais aussi tout autre élément, information ou circonstance ayant un contenu informatif susceptible de fournir des éléments de connaissance supplémentaires à l'égard d'une personne identifiée ou identifiable.
> Des données à caractère personnel peuvent donc se retrouver dans le cadre d'évaluations et jugements subjectifs, qui peuvent justement inclure des éléments spécifiques caractérisant l'identité physique, physiologique, mentale, économique, culturelle ou sociale de la personne concernée. Ceci vaut aussi lorsqu'un jugement ou une évaluation est exprimée sous forme de points, ou d'une échelle de valeurs, ou d'autres paramètres d'évaluation. Ceci peut revêtir une importance particulière lorsque le traitement de données personnelles est effectué dans le but d'évaluer l'aptitude des employés pour un poste déterminé, ce qui pourrait conduire à des discriminations ou bien à une évaluation incorrecte de l'employé sur base d'informations incomplètes »[18].

16. Quant au contenu des informations, il importe peu que les données soient publiques ou secrètes, qu'elles soient relatives à la sphère privée, publique ou professionnelle. Enfin, le support de l'information est également indifférent : l'information peut se trouver sur papier, sous format électronique ou numérique.

17. La donnée doit concerner une *personne physique*, à l'exclusion des personnes morales (sociétés, associations, personnes de droit public,…). En outre, les informations relatives à la famille d'un individu peuvent dans certaines circonstances être considérées comme des données à caractère personnel concernant cet individu. En ce sens, le Groupe de travail de l'Article 29 précise que « Les informations "concernent" une personne lorsqu'elles ont "trait" à cette personne, et une évaluation s'impose à la lumière de l'ensemble des circonstances du cas d'espèce. Par exemple, les résultats d'une analyse médicale concernent manifestement le patient, tout comme les informations contenues

---

17 Groupe de l'Article 29, Avis 4/2007 sur le concept de données à caractère personnel, WP 136, 20 juin 2007, p. 7, http://ec.europa.eu/justice/policies/privacy.

18 Groupe de l'Article 29, « Recommandation 1/2001 concernant les données d'évaluation des employés », WP 42, 22 mars 2001, p. 2, http://ec.europa.eu/justice/policies/privacy.

dans le dossier au nom d'un certain client concernent celui-ci »[19]. Le Groupe de travail de l'Article 29 indique encore en ce sens que « dans le cas de données enregistrées dans le dossier personnel d'un employé dans un service du personnel, il s'agit clairement de données "concernant" la situation de la personne en sa qualité d'employé »[20].

18. Pour être qualifiée de « donnée à caractère personnel », l'information doit concerner une personne *identifiée ou identifiable*, peu importe la nationalité de celle-ci. Autrement dit, sont considérées comme données à caractère personnel :

– les informations immédiatement liées à une personne identifiée.

  Ainsi toutes les informations qui sont associées à une personne identifiée sont des données à caractère personnel. Il peut s'agir, par exemple, des coordonnées d'un travailleur, de son adresse e-mail, de ses données fiscales et sociales, de son *curriculum vitae*, des rapports d'évaluation le concernant, de sa photographie, de son examen d'avancement, etc. ;

– les informations relatives à une personne dont on ne connaît pas l'identité mais qui pourrait, dans l'absolu, être identifiée soit par celui qui traite les données en question, soit par un tiers.

  À cet égard, l'article 1er de la loi du 8 décembre 1992 précise que « 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 ».
  Le considérant 26 de la directive 95/46/CE indique que pour déterminer si une donnée est ou non identifiable, il faut avoir égard aux moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne. Il s'agit donc d'une appréciation *in abstracto*, l'idée étant que si le responsable du traitement ne peut lui-même immédiatement trouver l'identité de la personne, un tiers pourrait être à même de la lui révéler.
  Sont ainsi considérées comme données à caractère personnel, une plaque d'immatriculation, les traces ADN, les images d'une bande vidéo même si l'on n'a pas identifié les personnes qui y apparaissent. Constituent également des données à caractère personnel les données codées c'est-à-dire les données qui ne peuvent être mise en relation avec une personne

[19] Groupe de l'Article 29, Avis 4/2007 sur le concept de données à caractère personnel, WP 136, 20 juin 2007, p. 11, http://ec.europa.eu/justice/policies/privacy.

[20] Groupe de l'Article 29, Avis 4/2007 sur le concept de données à caractère personnel, WP 136, 20 juin 2007, p. 10, http://ec.europa.eu/justice/policies/privacy.

identifiée ou identifiable que par l'intermédiaire d'un code[21]. Le fait qu'une adresse IP puisse être considérée comme donnée à caractère personnel est discuté. Le Groupe de l'Article 29 préconise que l'adresse IP soit considérée comme une donnée à caractère personnel lorsqu'il est possible qu'un lien puisse être établi entre une personne et l'adresse, le cas échéant par l'intermédiaire du fournisseur d'accès[22].

19. On oppose aux données à caractère personnel les données anonymes c'est-à-dire les données qui ne peuvent pas ou plus être mises en relation avec une personne identifiée ou identifiable[23]. Le traitement des données anonymes n'est soumis à aucune condition légale. En revanche, les opérations par lesquelles une donnée à caractère personnel est rendue anonyme constituent un traitement de données à caractère personnel et sont soumises au respect des conditions légales.

> Les données statistiques et agrégées sont typiquement des données anonymes, car elles ne permettent généralement plus l'individualisation et l'identification des personnes concernées à l'origine par ces données. Il n'est cependant pas exclu que des données statistiques puissent constituer des données à caractère personnel à partir du moment où une identification reste possible. Prenons l'exemple d'une enquête statistique réalisée au sein d'une entreprise et destinée à vérifier la corrélation entre l'utilisation de moyens de transport et les arrivées tardives le matin en entreprise. Si les résultats sont présentés département par département et que les paramètres choisis sont particulièrement identifiants parce qu'il est possible qu'une seule personne réponde à ce critère, il pourrait être aisé de trouver qui se cache derrière une donnée statistique. Par exemple, les résultats statistiques aux termes desquels sur le département RH, il y a un taux de retard de 15 % pour les personnes qui viennent au travail en moto ne sont pas des données anonymes s'il n'y a qu'une seule personne de ce département qui se rend au travail en moto, cette personne pouvant facilement être identifiée. Ces données doivent alors être traitées comme des données à caractère personnel[24].

2. Qu'entend-on par « traitement de données » ?

20. La notion de traitement de données à caractère personnel est très large. Elle recouvre « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère per-

---

21 Art. 1, 3° de l'A.R. du 13 février 2001.

22 Groupe de l'Article 29, Avis 4/2007 sur le concept de données à caractère personnel, WP 136, 20 juin 2007, p. 18, http://ec.europa.eu/justice/policies/privacy.

23 Art. 1, 5° de l'A.R. du 13 février 2001.

24 Commission de la protection de la vie privée, Avis 37/2001 concernant l'enquête socio-économique 2001, 8 octobre 2001, www.privacycommission.be.

sonnel, 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 »[25].

21. Bien que cela ne ressorte pas explicitement du texte de la loi, il nous semble que les termes « traitement de données » sont généralement utilisés pour désigner un ensemble d'opérations techniques qui poursuivent une ou plusieurs finalités définies. C'est ainsi que, d'un point de vue pratique, lorsqu'une personne doit déclarer un traitement de données à la Commission de la protection de la vie privée, il lui est proposé des catégories de finalités pour définir le traitement déclaré. Aussi parlera-t-on du traitement de données effectué par une entreprise pour la gestion de sa comptabilité pour englober toutes les opérations (enregistrement, suppression, communication,…) mises en œuvre dans le but de réaliser la comptabilité de l'entreprise.

3. Qu'entend-on par « fichier » ?

22. Un fichier est « 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 »[26]. Il peut s'agir tant d'un fichier électronique (sur ordinateur) que d'un fichier papier. Ce qui est déterminant pour la qualification de fichier papier, c'est l'existence d'une structure logique permettant le traitement systématique des données qui y sont contenues (consultation, diffusion, effacement,…). Ainsi, un simple dossier thématique qui ne permet pas ce traitement de données systématique ne peut être qualifié de « fichier » au sens de la loi du 8 décembre 1992[27].

B. Champ d'application matériel de la loi

23. La loi du 8 décembre 1992 s'applique à 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[28].

Avec l'avènement de l'utilisation de l'informatique, la loi devient incontournable : dès que des données à caractère personnel font l'objet d'un traitement de texte informatique, la loi trouve à s'appliquer. Elle ne s'appliquera pas

---

25 Art. 1er, § 2 de la loi du 8 décembre 1992.

26 Art. 1er, § 3 de la loi du 8 décembre 1992.

27 Cass., 16 mai 1997, *J.T.*, 1997, p. 779.

28 Art. 1, § 1 de la loi du 8 décembre 1992.

uniquement dans l'hypothèse où différentes opérations de traitement sur des données à caractère personnel interviennent sans qu'une opération informatique soit faite et sans que les données ne soient incluses dans un fichier papier.

> L'insertion de données à caractère personnel sur un site internet emporte application de la loi du 8 décembre 1992[29], tout comme l'usage du courrier électronique ou la communication de fichiers électroniques.
>
> La question de l'application de la loi du 8 décembre 1992 s'est également posée dans le cadre du dépistage par l'employeur de consommation de drogue et d'alcool dans le chef de travailleurs. La C.C.T. nº 100 prévoit en son article 4, 6° que « Le traitement des résultats de tests de dépistage d'alcool ou de drogues en tant que données personnelles dans un fichier est interdit ». Cette interdiction n'enlève rien au fait, selon nous, que dès lors que les résultats des tests font l'objet d'un traitement - ne serait-ce que partiellement automatisé -, la loi du 8 décembre 1992 sera applicable[30]. Autrement dit, le fait que l'on exclue le traitement dans le cadre d'un fichier n'implique pas que la loi ne trouvera pas à s'appliquer dans la mesure où les données seraient intégrées dans un traitement automatisé au sens de la loi.

Le contexte dans lequel le traitement de données a lieu est, quant à lui, indifférent de sorte que la loi s'applique tant aux autorités publiques qu'aux personnes morales de droit privé, aux associations de fait, etc., et ce indépendamment de l'activité menée[31].

Dès lors qu'un employeur traite, en tant que responsable de traitement, des données (informations écrites, photographies, images vidéo, empreintes digitales,…) relatives à ses travailleurs, qu'il s'agisse d'un enregistrement, d'une communication ou de la simple conservation de données à caractère personnel,

---

29 Arrêt de la C.J.C.E. 101/01 (dit arrêt *Bodil Lindqvist*), 6 novembre 2003, disponible sur le site http://curia.eu.int. L'arrêt *Lindqvist* C-101/01 de la C.J.C.E. a rappelé, à propos de la mise en ligne d'informations sur internet, que dès lors que l'on recourt à des moyens automatisés, il n'est pas nécessaire que les données soient rassemblées sous forme de fichier pour que la loi s'applique (C. DE TERWANGNE, « Affaire *Lindqvist* ou quand la Cour de justice des Communautés européennes prend position en matière de protection de données à caractère personnel », obs. sous C.J.C.E., 6 novembre 2003, *R.D.T.I.*, 2004, nº 19, p. 83).

30 Voy. en ce sens, P. DE HERT et R. SAELENS, « Oeps, de privacy vergeten », *Juristenkrant*, 27 mai 2009, p. 10.

31 Toutefois, la loi du 8 décembre 1992 ne s'applique pas lorsque le traitement est effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques (art. 3, § 2 de la loi du 8 décembre 1992). La loi contient également des exclusions partielles. Certaines des dispositions de la loi ne sont pas applicables aux traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire lorsque le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou sur des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée (*Cf.* art. 3, § 3 de la loi du 8 décembre 1992). D'autres exclusions partielles de la loi en considération de l'identité de l'auteur du traitement ont également été adoptées. De telles exemptions partielles sont en effet notamment prévues pour la sûreté de l'État (art. 3, § 4), les autorités publiques dans le cadre de leur missions de police judiciaire (art. 3, § 5) ou encore le Centre européen pour enfants disparus et sexuellement exploités (art. 3, § 6).

il est tenu de se conformer aux conditions qui permettent de garantir la transparence et la légitimité des traitements.

Section 2
La loi belge est-elle applicable ?

24. Il existe deux critères d'application territoriale. Le critère principal retenu pour l'application de la loi du 8 décembre 1992 est le lieu d'établissement du responsable du traitement sur le territoire belge dans le cadre des activités duquel le traitement est effectué (point A.). Si le responsable de traitement n'est pas localisé sur le territoire belge, la loi belge sera tout de même applicable dans la mesure où le responsable de traitement fait usage de moyens localisés sur le territoire belge pour mettre en œuvre le traitement de données (point B.).

A. Critère du lieu d'établissement du responsable du traitement

25. La loi du 8 décembre 1992 s'applique lorsque le traitement est 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[32].

1. Qui est le responsable du traitement ?

26. La loi du 8 décembre 1992 distingue plusieurs acteurs dans le cadre de traitement de données. Outre le responsable de traitement, la loi définit les notions de « tiers »[33], de « destinataire » et de « sous-traitant ». C'est souvent à la notion de sous-traitant que l'on oppose celle de responsable du traitement, le sous-traitant étant la personne qui, sans être placée sous l'autorité directe du responsable du traitement, traite des données à caractère personnel pour le compte de ce dernier[34].

27. Il est primordial de pouvoir déterminer qui est le responsable du traitement (anciennement appelé « maître de fichier » sous la mouture de la loi du 8 décembre 1992 avant sa révision de 1998), et ce d'autant plus que c'est à

---

32 Art. 3*bis*, 1°, de la loi du 8 décembre 1992.

33 Le terme « tiers » vise les personnes qui ne sont pas impliquées dans le traitement de données tandis que le terme « destinataire » désigne les personnes à qui les données sont communiquées, que ces destinataires soient ou non par ailleurs tiers au traitement (art. 1, §§ 6 et 7 de la loi du 8 décembre 1992). Ainsi, le département d'une entreprise peut être considéré comme destinataire de données quand bien même il ne s'agit pas d'un tiers puisqu'il dépend de l'entreprise responsable du traitement (Exposé des motifs de la loi du 8 décembre 1992, *Doc. Parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 16).

34 Art. 1, § 5 de la loi du 8 décembre 1992.

lui qu'incombent, par ailleurs, la plupart des obligations définies par la loi du 8 décembre 1992. Il convient de distinguer à cet égard deux hypothèses :

a. *Le traitement est prévu dans un texte légal :* dans ce cas la loi du 8 décembre 1992 dispose que « lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le responsable du traitement est la personne physique, la personne morale, l'association de fait ou l'administration publique désignée comme responsable du traitement par ou en vertu de cette loi, de ce décret ou de cette ordonnance »[35].

b. *Dans tous les autres cas :* le responsable du traitement est « 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 »[36].

La qualité de responsable de traitement dépend donc, dans ce second cas, d'une situation de fait : il convient pour chaque traitement de déterminer qui se charge ou a le pouvoir de décider des finalités du traitement ainsi que des moyens mis en œuvre pour le réaliser. Il peut s'agir de plusieurs personnes lorsqu'elles participent toutes à la détermination des finalités et des moyens de traitement. Dans ce cas, elles sont coresponsables de traitement.

Il est possible de déterminer dans un contrat qui sera le responsable d'un traitement. Dans ce cas, il est convenu entre parties que la personne désignée aura le pouvoir de décision et assumera les responsabilités qui incombent à un responsable de traitement. Ceci étant, il conviendra toujours d'avoir égard à la situation de fait. S'il s'avère que dans les faits, c'est une autre personne qui détermine les finalités et moyens de traitement, cette dernière sera considérée comme la responsable du traitement aux yeux des tiers. En effet, la loi du 8 décembre 1992 étant d'ordre public, on ne peut choisir par contrat de désigner comme responsable de traitement une autre personne que celle qui s'impose au regard des critères définis par la loi du 8 décembre 1992.

28. Il n'est pas toujours aisé de déterminer qui est le responsable du traitement.

À titre d'illustration, prenons l'exemple d'un projet dans lequel différentes entités sont impliquées. Plusieurs cas de figure peuvent se présenter :

a. En cas de projet confié par une entité A à une entité B, qui est responsable des traitements de données à caractère personnel mis en œuvre pour l'exécution du projet ?

L'entité A ne sera le responsable du traitement que dans la mesure où c'est elle qui définit concrètement les finalités et les moyens de traitement. Cela dépendra de

35 Art. 1er, § 4 de la loi du 8 décembre 1992.

36 *Idem.*

la marge de manœuvre laissée à l'entité B. Dans bien des cas, c'est l'entité exécutante qui prend en main l'exécution du projet et sera la responsable du traitement.

b. En cas de projet exécuté par différentes entités, qui est le responsable des traitements mis en œuvre pour l'exécution du projet ?

On doit distinguer deux hypothèses à cet égard :

- Soit l'ensemble des traitements effectués par les participants au projet forment un tout cohérent, auquel cas ce sont le ou les partenaires qui décident des finalités et moyens de traitement qui sont le ou les responsables de traitement. Les autres sont éventuellement des sous-traitants[37].
- Soit les traitements sont distincts et chaque partenaire est responsable des traitements de données à caractère personnel qu'il effectue pour la mise en œuvre de la partie du projet qui lui est confiée.

2. Qu'implique l'exigence aux termes de laquelle le traitement doit intervenir dans le cadre des activités d'un établissement situé sur le territoire belge ?

29. Un établissement suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable tandis que la forme juridique du responsable de traitement et l'existence ou non d'une personnalité juridique importent peu[38].

Pour déterminer si c'est la loi belge qui s'applique à un établissement (siège, filiale ou succursale), il convient donc de vérifier si c'est bien dans le cadre des activités de celui-ci que le traitement est effectué[39].

Imaginons que, dans un groupe de sociétés, les données relatives à l'évaluation du travail des cadres d'une succursale belge sont communiquées à la société mère localisée aux États-Unis où sont prises des décisions relatives aux promotions. On devra considérer que c'est bien dans le cadre des activités de la succursale belge que le traitement a lieu et que la loi belge est applicable.

30. S'il y a plusieurs responsables pour un même traitement et que ceux-ci sont établis dans différents États membres de l'Union européenne dont la Belgique, le traitement devra être conforme aux exigences de chacune des lois relatives à la protection des données de ces États membres et donc également à la loi belge.

---

37 Voir *supra* n° 26 et suiv. pour une définition de cette notion.

38 Voy. à cet égard le considérant 19 de la directive 95/46/CE auquel se réfère l'exposé des motifs de la loi du 8 décembre 1992 (Exposé des motifs, *Doc. Parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 27).

39 Th. Léonard voit également une autre condition implicite à l'application de la loi belge, à savoir que l'établissement en question participe lui-même au traitement de données (Th. Léonard, « La protection des données à caractère personnel et l'entreprise », *Guide Juridique de l'Entreprise*, Titre XI, Livre 112.1, Bruxelles, Kluwer, 2004, 2e éd., p. 23). Le Groupe de l'article 29 a élaboré un avis daté du 16 décembre 2010 et qui fait une analyse détaillée de la manière selon laquelle le critère de la localisation du lieu de l'établissement dans le cadre duquel le traitement a lieu devrait être interprété (Groupe de l'Article 29, « Opinion 8/2010 on applicable law », WP179, 16 décembre 2010, p. 8-17, http://ec.europe.eu/justice/policies/privacy).

B. Critère des moyens utilisés

31. En sus du critère d'établissement, l'article 3*bis*, 2° de la loi impose un second critère d'application territorial. La loi belge s'applique, nonobstant le fait que le responsable de traitement n'a pas d'établissement sur le territoire de l'Union européenne, s'il « 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 ». Le responsable du traitement doit alors désigner un représentant établi sur le territoire belge, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même[40].

Ce faisant, le législateur belge a transposé, presque mot pour mot, l'article 4, 1., c) de la directive 95/46/CE. Le but de cette disposition est d'éviter de voir le responsable du traitement tenter de contourner les législations européennes applicables en s'établissant en dehors du territoire européen alors même que le traitement porte sur des données qui en proviennent et que le bénéfice de ce traitement est à rechercher dans ses activités orientées vers l'Union européenne.

C'est donc l'utilisation de moyens localisés sur le territoire auxquels on recourt pour mettre en œuvre un traitement qui entraîne l'applicabilité de la loi belge en particulier, et des lois européennes en général. Dès lors que le responsable n'a pas d'établissement sur le territoire communautaire mais utilise n'importe quel moyen situé sur le territoire belge en vue de traiter des données à caractère personnel[41], la loi belge s'applique sous réserve du seul transit des données sur le territoire[42]. L'exposé des motifs de la loi belge paraît aller en ce sens[43]. Certains commentateurs également[44].

> La portée exacte de ce critère n'est pourtant pas claire et pose de sérieuses difficultés en pratique. La principale difficulté provient du fait que, vue l'in-

---

40 Art. 3*bis*, 2°, de la loi du 8 décembre 1992.

41 Ou qu'il dispose d'un tel établissement mais que le traitement n'est pas effectué dans le cadre des activités de cet établissement.

42 Pour une analyse de cette problématique appliquée aux sites internet, voy. Groupe de l'Article 29, « Document de travail sur l'application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur internet par des sites web établis en dehors de l'UE », WP 56, 30 mai 2002, http://ec.europa.eu/justice/policies/privacy, voy. également Groupe de l'article 29, « Opinion 8/2010 on applicable law », WP179, 16 décembre 2010, pp. 10-25, http://ec.europe.eu/justice/policies/privacy.

43 D'après l'exposé des motifs de la loi du 8 décembre 1992, « Le terme « moyens » recouvre tout équipement possible, tels que les ordinateurs, les appareils de télécommunication, les unités d'impression, etc., à l'exclusion, formulée explicitement, des moyens qui sont uniquement utilisés pour le transit des données à caractère personnel par le territoire, tels que les câbles, les routeurs, etc. » (Exposé des motifs, *Doc. Parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 27).

44 J. Dumortier, « De nieuwe wetgeving over de verwerking van persoonsgegevens », *in Recente ontwikkelingen in informatica- en telecommunicatierecht*, Brugge, Die Keure, 1999, p. 85, spéc. note 33.

> ternationalisation croissante des traitements de données, il sera très souvent possible de considérer que le responsable établi en dehors de l'Union européenne utilise des moyens qui y sont situés pour les besoins de ses traitements. L'application de ce critère peut dès lors avoir des effets surprenants. Prenons l'exemple d'un responsable de traitement établi hors de l'Union européenne et qui confie des prestations techniques de traitement de données collectées dans son propre pays à un sous-traitant établi sur le territoire belge. Il pourrait être considéré que, ce faisant, ce responsable de traitement recourt à des moyens localisés en Belgique pour traiter des données à caractère personnel. La loi belge doit donc s'appliquer si l'on s'en tient à une interprétation stricte du critère, quand bien même cette application extraterritoriale de la loi belge peut paraître incongrue[45].

Section 3
Le traitement envisagé est-il ou non régi par la loi du 8 décembre 1992 ?

32. Il convient de noter que la loi du 8 décembre 1992 prévoit une série d'hypothèses dans lesquelles elle ne s'applique pas, en tout ou en partie[46]. Il convient de s'assurer que ces hypothèses ne sont pas rencontrées avant de conclure à l'application de la loi.

Étape 2
Déterminer si le traitement envisagé est licite au regard des exigences de la loi du 8 décembre 1992

33. Dans l'hypothèse où l'on identifie un traitement de données à caractère personnel soumis à la loi du 8 décembre 1992, on se doit de vérifier si le traitement peut être mis en œuvre au regard des restrictions prévues par la loi.

Nous nous limiterons à ce stade aux obstacles qui interdiraient que le traitement puisse être mis en œuvre. Ces obstacles peuvent être liés à la finalité d'utilisation envisagée (*cf.* section 1, *infra*), à la nature des données dont le traitement est envisagé (*cf.* section 2, *infra*) ou encore aux opérations de traitement envisagées (*cf.* section 3, *infra*).

---

45 Voy. sur cette question, Th. Léonard et A. Mention, « Transferts transfrontaliers de données : quelques considérations théoriques et pratiques », *in Actualités du droit de la vie privée*, Bruxelles, Bruylant, 2008, pp. 113.

46 Voy. *supra*, note de bas de page nº 31.

Section 1
Obstacles liés à la finalité d'utilisation

34. En application de la loi du 8 décembre 1992, les données à caractère personnel ne peuvent être recueillies qu'en vue d'une ou de plusieurs *finalités déterminées, explicites et légitimes*[47].

1. *Des finalités déterminées* : on ne peut pas collecter des données à caractère personnel et décider d'utiliser ces données sans un but précis. C'est ce but décidé au départ qui va orienter toute la suite des opérations. C'est, en effet, en fonction de l'objectif poursuivi que l'on saura quelles données on peut collecter, ce que l'on peut faire avec ces données, si on peut les communiquer et à qui, etc.
2. *Une ou plusieurs finalités explicites :* le responsable du traitement ne peut tenir les finalités poursuivies secrètes. Il doit les indiquer aux personnes concernées (obligation d'information) et les déclarer à la Commission de la protection de la vie privée (obligation de déclaration)[48].
3. *Une ou plusieurs finalités légitimes* : pour que le traitement puisse être admis, chaque finalité que le responsable poursuit en traitant des données à caractère personnel doit être légitime. Cela implique qu'un équilibre existe entre l'intérêt du responsable du traitement et les intérêts des personnes sur qui portent les données traitées. On n'admettra pas comme légitime un objectif qui causerait une atteinte excessive aux droits et libertés des personnes concernées.
   Le législateur a prévu différents cas de figure dans lesquels le traitement est *a priori* légitime. Ceux-ci sont des causes de justification sociale qui seront examinées ci-après. De même, on peut considérer que le traitement est *a priori* légitime s'il s'inscrit dans le cadre des exceptions prévues pour le traitement des données sensibles sur lequel nous reviendrons *infra*.

35. Nous retiendrons deux conséquences de l'application des principes susmentionnés qui ont une incidence sur la légalité de la mise en œuvre du traitement :

A. Le traitement doit s'inscrire dans l'une des causes de justification sociale prévues par la loi du 8 décembre 1992

36. En sus d'exigence de légitimité de traitement, les données à caractère personnel ne peuvent être traitées que si le responsable du traitement peut

47 Art. 4, §1er, 2° de la loi du 8 décembre 1992.
48 *Cf.* nº 72 et suiv., Étape 3, section 2.

s'appuyer sur au moins une des causes de justification sociale définies par la loi et dont les plus pertinentes dans le cadre de la relation de travail sont les suivantes[49] :

– si le traitement des données est nécessaire à l'exécution d'un *contrat* ou à l'exécution de mesures précontractuelles sollicitées par la personne concernée.
  Cette base de légitimité permettra à l'employeur de mettre en œuvre la plupart des traitements de données qui sont liés à l'exécution même du contrat de travail : l'établissement d'un contrat de travail, l'administration des salaires, le traitement des données dans le cadre du suivi des tâches du travailleur, etc. ;

– ou si le traitement est exigé par une *loi, un décret ou une ordonnance*.
  Ainsi en est-il des traitements de données qu'implique l'application de la législation en matière de sécurité sociale, à commencer par la déclaration DIMONA prévue par l'arrêté royal du 5 novembre 2002 instaurant une déclaration immédiate de l'emploi, en application de l'article 38 de la loi du 26 juillet 1996 portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux des pensions.
  Notons que dans un avis portant sur les systèmes d'alerte interne professionnelle (ou *whistleblowing*), la Commission de la protection de la vie privée a considéré que « Pour pouvoir parler d'une obligation légale au sens de l'article 5, c) de la LVP en respect de laquelle une organisation est tenue de traiter des données à caractère personnel via un système d'alerte, il doit s'agir d'une disposition légale du droit belge. Une obligation légale étrangère ne peut pas entrer ici en ligne de compte. La Commission partage à cet égard le point de vue du Groupe de l'Article 29 et des Commissions de protection de la vie privée française et néerlandaise »[50] ;

– ou, si le traitement des données est nécessaire pour réaliser un *intérêt légitime* du responsable ou d'un tiers, à condition que l'intérêt ou les droits de la personne concernée ne prévalent pas. Des traitements sont admis si l'intérêt du responsable du traitement à traiter les données est supérieur

---

49 Art. 5 de la loi du 8 décembre 1992 ; voy. ég. Groupe de l'Article 29, Avis 2001/8 sur le traitement des données à caractère personnel dans le contexte professionnel, WP 48, 13 septembre 2001, p. 17, http://ec.europa.eu/justice/policies/privacy.

50 Commission de la protection de la vie privée, « Recommandation n° 1/2006 relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel », 29 novembre 2006, p. 4, www.privacycommission.be.

à l'intérêt de la personne concernée à ce que ses données ne soient pas traitées.

> Cette base de justification qui a une application plus large et plus incertaine que les autres en ce qu'elle implique une balance ponctuelle des intérêts en présence, peut, le cas échéant, servir de base à des traitements qui, sans qu'ils ne soient exigés par la loi ni qu'ils ne s'imposent en vue de l'exécution du contrat de travail, présentent un intérêt pour l'employeur. Ainsi en est-il des évaluations des membres du personnel ou de certains contrôles opérés sur les travailleurs qui se justifient au regard des obligations du travailleur de respecter les instructions de l'employeur dans le cadre du contrat de travail.

– si la personne concernée a sans ambiguïté donné son *consentement*. Le consentement n'est valable que s'il est libre (c'est-à-dire s'il a été émis sans pression), spécifique (le consentement doit porter sur un traitement précis) et informé (la personne a reçu toute l'information utile sur le traitement envisagé). Le consentement ne doit pas nécessairement être donné par écrit.

> Le consentement n'est donc qu'une des causes de justification sociale envisagées par le législateur et ne doit pas d'office être obtenu pour effectuer un traitement de données. Il est toutefois indispensable lorsqu'aucune autre base ne peut être utilement invoquée pour fonder un traitement de données. Ainsi en serait-il, à notre estime, de l'annonce à l'ensemble des membres du personnel d'informations à caractère privé relatives à un travailleur, telle la publication d'un avis de naissance d'un enfant d'un travailleur sur l'intranet de l'entreprise.

Ceci étant, tant le législateur belge (à propos du traitement des données sensibles) que le Groupe de travail l'Article 29 conçoivent des doutes quant à la possibilité de considérer qu'un travailleur pourrait donner un consentement libre dans le contexte de la relation de travail.

L'article 27 de l'arrêté royal du 13 février 2001 prévoit que « Lorsque le traitement de données à caractère personnel, visées aux articles 6 et 7 de la loi [du 8 décembre 1992], est exclusivement autorisé par le consentement écrit de la personne concernée, ce traitement est, néanmoins, interdit 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 ». Il est toutefois précisé que « Cette interdiction est levée lorsque le traitement vise l'octroi d'un avantage à la personne concernée ».

Par ailleurs, dans un avis du 13 septembre 2001, le Groupe de l'Article 29 estime que le consentement ne devait être considéré comme possible

base de traitement que si aucune autre cause de justification n'était envisageable. Il précise dans la foulée que « si le consentement du travailleur est nécessaire et que l'absence de consentement peut entraîner un préjudice réel ou potentiel pour le travailleur, le consentement n'est pas valable au titre de l'article 7 ou de l'article 8 [de la directive 95/46/CE], dans la mesure où il n'est pas donné librement. Si le travailleur n'a pas la possibilité de refuser, il ne s'agit pas de consentement. Le consentement doit toujours être donné librement. En conséquence, le travailleur doit avoir la possibilité de se dégager de son consentement sans préjudice »[51]. Aussi, pour pallier ce type d'écueil, T. Van Overstraeten préconise-t-il d'assortir le consentement individuel du travailleur d'une procédure d'acceptation générale dans l'entreprise par le biais de l'adoption d'un règlement de travail[52].

À défaut de pouvoir se fonder sur l'une des hypothèses visées par la loi, le traitement ne peut être mis en œuvre.

B. Les opérations de traitement doivent s'inscrire dans le cadre de la finalité de traitement initialement définie ou ne pas être incompatibles avec celle-ci

37. Un second corollaire du principe de finalité est que le responsable du traitement ne peut traiter des données à caractère personnel que dans la mesure ou ces traitements s'inscrivent dans la ou les finalités initialement poursuivies ou ne sont pas incompatibles avec ces finalités. Par exemple, le transfert de données par un responsable de traitement à un tiers doit être compatible avec les finalités initiales. Si tel ne devait pas être le cas, il faudrait considérer que ce traitement est illicite[53].

Le terme « compatible » n'est pas défini par la loi du 8 décembre 1992. Pour déterminer ce qui est « compatible », précise l'article 4, 2° de cette loi, il y a lieu de tenir compte de tous les facteurs pertinents, notamment des prévisions raisonnables de la personne concernée et des dispositions légales réglementaires applicables. On comprend, à la lecture des commentaires qui sont réservés à cette disposition dans les travaux préparatoires[54], qu'il y a lieu de parler

---

51 Groupe de l'Article 29, Avis 2001/8 sur le traitement des données à caractère personnel dans le contexte professionnel, WP 48, 13 septembre 2001, pp. 31-32, http://ec.europa.eu/justice/policies/privacy.

52 T. Van Overstraeten, « La protection des données à caractère personnel : quelques réflexions de praticien », *in Les 25 marchés émergents du droit*, (dir. L. Marlière), Bruxelles, Bruylant, 2006, p. 363.

53 Comm. Bruxelles, 12 juillet 1996, *D.C.C.R.*, 1996, p. 351.

54 Les travaux parlementaires de la loi du 8 décembre 1992 apportent certaines précisions utiles quant à ce deuxième critère : « Afin de vérifier si un traitement est compatible avec la finalité pour laquelle les don-

de « réutilisation de données » lorsqu'il s'agit d'entamer un nouveau traitement sur des données dont le responsable du traitement ou le tiers qui lui fournit les données dispose d'ores et déjà. Toute autre est la situation dans laquelle le responsable du traitement collecte des informations en ayant à l'esprit différentes finalités d'utilisation, que celles-ci soient d'ailleurs compatibles ou incompatibles entre elles : en vertu du devoir de loyauté, il lui faudra informer les personnes concernées relativement à toutes les finalités d'utilisation[55].

Il convient donc de rester très prudent lorsqu'il s'agit par exemple de communiquer des données à caractère personnel à des tiers. Ces communications constituent des traitements de données à part entière, ce qui implique qu'elles ne sont légitimes que dans la mesure où elles s'inscrivent dans le cadre d'une finalité pour laquelle les données ont été collectées initialement ou, à tout le moins compatible avec celle-ci.

Ces exigences s'appliquent pleinement en ce qui concerne les données relatives au personnel du responsable du traitement. Si certaines utilisations entrent implicitement, mais certainement dans le cadre de l'exécution du contrat de travail, il en est d'autres qui ne vont pas de soi et qui devront faire l'objet d'une information suffisamment claire et précise.

> Ainsi, il paraît évident que les données collectées au moment de l'engagement concernant l'identité du travailleur, sa date de naissance, son adresse personnelle seront utilisées dans le cadre de l'administration du personnel pour lui adresser la correspondance relative au contrat de travail, pour l'établissement de ses fiches de paie ou encore dans le cadre d'un licenciement.
>
> En revanche, si d'autres traitements envisagés peuvent détromper les attentes raisonnables et légitimes du travailleur, il importera de s'assurer, dès l'engagement d'une nouvelle personne, de ces finalités d'utilisation des données collectées que l'employeur envisage de faire et d'en informer la personne concernée. Une telle incompatibilité peut se rencontrer lorsqu'une entreprise communique des données à d'autres entités d'un même groupe de sociétés,

---

nées ont été collectées, il conviendra parfois de tenir compte de dispositions légales ou réglementaires. Il est notamment possible que les autorités souhaitent utiliser certaines données à caractère personnel concernant les citoyens pour une nouvelle finalité inconnue lors de la collecte des données relatives à l'immatriculation des véhicules pour mettre en œuvre un système relatif au permis à points. Il est évident que, si les autorités disposent déjà des données nécessaires pour cette nouvelle finalité, elles ne sont pas obligées de redemander ces données aux personnes concernées. Dans un cas pareil également, la mesure dans laquelle et la manière dont les personnes concernées ont préalablement été informées du nouveau traitement par les autorités jouera un rôle important lors de l'évaluation de la compatibilité ou de l'incompatibilité du traitement avec la finalité initiale pour laquelle les données ont été obtenues. Il convient cependant d'observer que l'information de la personne concernée n'est pas obligatoire si l'enregistrement ou la communication des données à caractère personnel sont prévus par la loi (considérant 40 de la directive) » (Exposé des motifs, *Doc. Parl.*, Ch. Repr., sess. ord. 1997-1998, 1566/1-n° 1, pp. 29 et 30).

55 (*cf. infra* n° 78 et suiv.).

met sur le site internet voire sur un site Intranet de l'entreprise le CV d'un collaborateur, ou encore intègre les coordonnées privées du travailleur dans un trombinoscope distribué à l'ensemble du personnel.

Si un nouveau traitement est envisagé en cours de contrat, il faut en principe procéder à une nouvelle collecte d'informations en respectant les conditions définies par la loi dans la mesure où la loi du 8 décembre 1992 n'autorise pas la réutilisation de données à des fins incompatibles avec les finalités initiales de traitement[56].

À titre d'illustration, si l'employeur a fait disposer une photographie sur les badges d'accès de travailleurs, il s'agit d'assurer un contrôle efficace de l'accès aux locaux de l'entreprise et d'en assurer la sécurité. Il ne peut être question de réutiliser la photographie ainsi obtenue à d'autres fins, par exemple, en la faisant figurer dans une brochure publiée pour promouvoir l'entreprise[57].

Section 2
Obstacles liés à la nature des données traitées

38. Si toutes les données peuvent, dans l'absolu, faire l'objet d'un traitement, il existe certaines catégories de données qui, sauf exceptions, ne peuvent être traitées.

Il s'agit des données sensibles et d'autres données qui font l'objet de réglementations particulières.

A. Données sensibles

39. Certaines données sont des informations personnelles par nature beaucoup plus sensibles que d'autres. Alors que le nom et l'adresse de quelqu'un sont des informations somme toute anodines, il n'en est pas de même des

---

56 Mis à part dans le cadre du régime spécifique défini dans l'A.R. du 13 février 2001 relatif aux traitements à des fins historiques, scientifiques ou statistiques.

57 À noter que la Commission de la protection de la vie privée adopte une position plus souple à cet égard en considérant que « la photo d'un employé prise pour la confection d'un badge d'identification ne pourra pas figurer sur un site intranet ou encore apparaître dans une brochure éditée par l'employeur sans qu'un accord explicite de l'employé pour ces autres finalités n'ait été demandé de manière concomitante au moment de la confection du badge ou ultérieurement lors de la mise sur intranet ou de la publication dans une brochure » (Commission de la protection de la vie privée, Avis d'initiative N° 02 / 2004 relatif aux badges d'identification sur lesquels figurent le nom et/ou la photo du détenteur du badge, 26 février 2004, p. 3, www.privacycommission.be). Cette position, aux termes de laquelle une réutilisation des données serait possible moyennant le consentement de la personne concernée nous semble contraire à la loi, bien qu'elle ait été préconisée par Y. Poullet et Th. Léonard (Y. Poullet et Th. Léonard, « La protection des données à caractère personnel en pleine (r)évolution », *J.T.*, 1999, n° 31, p. 385).

convictions politiques de cette personne, de ses préférences sexuelles ou de son passé judiciaire. La loi du 8 décembre 1992 règle de manière beaucoup plus stricte l'enregistrement et l'utilisation de ces informations sensibles.

Tandis que le traitement des données « ordinaires » est permis pour autant que certaines conditions prévues par la loi soient remplies, le traitement des données sensibles est interdit sauf dans le cas des exceptions limitativement prévues par la loi. Et même dans le cas où le traitement entre dans le champ d'application d'une de ces exceptions, il reste soumis aux mêmes conditions que le traitement des données « ordinaires ».

1. Quelles données sont considérées comme sensibles ?

40. Les données sensibles rassemblent une série de données à caractère personnel dont le législateur a estimé qu'elles touchaient davantage à la vie privée et dont le traitement devait dès lors être réservé à des hypothèses restreintes.

En droit belge, les données sensibles se subdivisent, dans leur réglementation légale, en trois groupes :

a. Les données relatives à la santé

41. Il s'agit tant des données relatives à l'état de santé que celles ayant trait à des pathologies particulières, qu'elles soient mentales ou physiques, et ce indépendamment du fait qu'il s'agisse de l'état de santé actuel, antérieur ou futur de la personne concernée[58].

Dans un arrêt du 6 novembre 2003, la Cour de justice de l'Union européenne a jugé que l'indication du fait qu'une personne s'est blessée au pied et est à temps partiel pour raisons médicales constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, § 1, de la directive[59]. Le Groupe de l'Article 29 a, quant à lui, considéré comme constituant des données relatives à la santé les données à caractère personnel qui présentent un lien clair et étroit avec la description de l'état de santé d'une personne, les données sur la consommation de médicaments, d'alcool ou de drogue et les données génétiques[60].

---

58 Voy. à cet égard : Commission de la protection de la vie privée, Avis d'initiative nº 08/2002 relatif au traitement de données à caractère personnel réalisé par des sociétés privées d'intérim, 11 février 2002, p. 2, www.privacycommission.be.

59 C.J.C.E., arrêt *Bodil Lindqvist* du 6 novembre 2003, affaire C-101/01.

60 Groupe de l'Article 29, « Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME) », 15 février 2007, p. 8, http://ec.europa.eu/justice/policies/privacy.

42. Les données relatives à la santé correspondent à des données qui *se rapportent* à la santé d'une personne. Le simple fait qu'une information *révèle* une donnée relative à la santé ne suffit donc pas[61]. Ainsi une photographie qui révèlerait le handicap d'une personne n'est pas une donnée relative à la santé[62]. On pourrait toutefois nuancer cette interprétation en précisant que, si la photographie fait l'objet d'un traitement pour les données relatives à la santé qu'elle révèle, elle doit alors être considérée comme une donnée sensible. En ce sens, la Commission de la protection de la vie privée a estimé que si une donnée biométrique (image, empreintes,…) utilisée pour le contrôle d'accès n'est *a priori* pas une donnée relative à la santé ; en revanche, lorsque elle est utilisée pour en déduire une information relative, par exemple à l'état de santé ou l'origine raciale, cette donnée doit être considérée comme une donnée sensible[63].

b. Les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la vie sexuelle

43. Si l'on s'en tient à la terminologie utilisée, les données qui appartiennent à ces catégories ne se limitent pas à celles qui révèlent immédiatement l'information sensible. Elles concernent également toutes les données dont on peut raisonnablement déduire une information *révélant* des données sensibles.

Ainsi l'information « M. Robert est de confession juive » est une donnée sensible, tout comme l'information « M. Robert prend des repas cascher » puisqu'on peut raisonnablement déduire l'appartenance religieuse de M. Robert. Il en est de même de l'information selon laquelle un individu paie une cotisation à un syndicat. En revanche, la Cour d'appel de Bruxelles a considéré que l'information selon laquelle les coordonnées électroniques d'une personne se trouvent reprises dans le fichier utilisé pour communiquer sur les activités du Front National n'est pas de nature à *révéler* les opinions politiques de cette personne lorsque les coordonnées d'autres personnes s'y trouvent également reprises en raison de leurs intérêts professionnels (tels des journalistes), par sympathie ou par simple curiosité[64]. Dans un tel cas, on ne peut inférer de cette appartenance au fichier une information relative à une appartenance à un

---

61 Exposé des motifs de la loi du 8 décembre 1992, *Doc. Parl.*, Ch. Repr., sess. ord. 1997-1998, 1566/1 n° 1, p. 34. M. De Bot va même plus loin en affirmant que pour être qualifiées comme telles, les données relatives à la santé doivent porter directement sur la santé ou l'état de santé d'une personne (D. De Bot, *Verwerking van persoonsgegevens*, Antwerpen, 2001, Kluwer, p. 154).

62 Y. Poullet et Th. Léonard, « La protection des données à caractère personnel en pleine (r)évolution », *J.T.*, 1999, n° 38, p. 387.

63 Commission de la protection de la vie privée, Avis d'initiative n° 17/2008 relatif aux traitements de données biométriques dans le cadre de l'authentification de personnes (A/2008/017), 9 avril 2008, p. 8, www.privacycommission.be.

64 Bruxelles (11e ch.), 17 mars 2010, *Dr. pén. entr.*, 2010/4, p. 319, note K. Rosier.

parti politique ou une adhésion à des opinions politiques et la donnée n'est pas une donnée sensible.

44. Il reste que la définition donnée par la loi peut s'avérer trop large si on l'applique à la lettre. On pourrait ainsi considérer que le nom patronymique est susceptible dans certains cas de donner une indication sur l'origine ethnique de la personne qui le porte. Il en est de même de certains titres attachés à une fonction ecclésiastique qui révèlent les convictions religieuses de la personne concernée. Nous considérons qu'il faut privilégier une interprétation raisonnable de la loi et avoir égard au contexte de l'utilisation de telles données. Le nom patronymique d'un individu ne doit pas être considéré en tant que tel comme une donnée sensible sauf s'il ressort du contexte dans lequel il est traité qu'il en est inféré une information sur les origines ethniques ou raciales d'un individu. C'est en ce sens nous semble-t-il que la Commission de la protection de la vie privée a analysé le traitement de données relatives à la nationalité d'une personne, de ses parents et grands-parents comme étant des données sensibles dans la mesure où ces données étaient traitées dans le but de mettre en œuvre une politique d'égalité des chances et de diversité dans la gestion des ressources humaines[65]. Dans la droite ligne de ce qui précède, la nationalité d'une personne ne nous semble pas être en soi une donnée sensible. Toujours dans le même sens, la Commission estime, après avoir relevé que « certaines données biométriques peuvent révéler des informations sur l'état de santé ou l'origine raciale d'un individu », que cette donnée devra être considérée comme sensible « lorsque les données biométriques sont utilisées pour en déduire une information relative, par exemple à l'état de santé ou l'origine raciale, ces données doivent être considérées comme des données sensibles »[66]. Autrement dit, si on suit le raisonnement de la Commission, le fait qu'une donnée révèle des informations sur l'origine raciale d'une personne ne semble pas déterminant pour la qualifier de sensible, encore faut-il qu'il y ait usage de la donnée pour cette information qu'elle révèle.

45. On ne peut manquer de constater que la loi utilise une autre terminologie en ce qui concerne la dernière catégorie de données qu'elle évoque : les données *relatives* à la vie sexuelle. À l'instar de ce qui a été dit concernant les données relatives à la santé, il nous semble qu'il y a lieu de considérer que ne tombent en toute hypothèse dans cette catégorie que les données qui se rap-

---

65 Commission de la protection de la vie privée, Avis n° 07 relatif au projet « monitoring des 'groupes à potentiel' au sein du fichier du personnel du Ministère de la Communauté flamande géré via le système 'Vlimpers' », 22 mars 2006, www.privacycommission.be.

66 Commission de la protection de la vie privée, Avis d'initiative n° 17/2008 relatif aux traitements de données biométriques dans le cadre de l'authentification de personnes (A/2008/017), 9 avril 2008, p. 8, www.privacycommission.be.

portent à la vie sexuelle des personnes qu'elles concernent. Il ne suffit donc pas qu'on puisse inférer d'une donnée l'existence d'indications sur la vie sexuelle d'une personne mais qu'il faudrait en outre, pour que la donnée soit qualifiée de sensible, qu'elle soit traitée pour l'information qu'elle donne sur la vie sexuelle de la personne concernée. Ainsi, le fait qu'on enregistre dans le cadre de la gestion des salaires le nom de l'époux ou de l'épouse ne suffit pas à considérer qu'il s'agit là de données relatives à la vie sexuelle de la personne concernée en ce qu'elles permettent de conclure à l'hétérosexualité ou l'homosexualité de celle-ci. En revanche, si ces mêmes données sont traitées pour cette information qu'elles révèlent elles devront être considérées comme sensibles.

c. Les données à caractère personnel 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 («données judiciaires»)

46. Cette catégorie de données est relativement large en ce qu'elle ne concerne pas uniquement les données relatives à des décisions judiciaires mais également les données relatives à des suspicions d'infractions pénales. Des données concernant des suspicions de fraude de la part de la clientèle et enregistrées dans des banques de données privées de commerçants concernent des données judiciaires[67]. Il en est de même des données relatives à des suspicions d'infraction commises par les membres du personnel traitées dans le cadre de systèmes d'alerte interne à l'entreprise (système auquel il est également référé par le terme «Whistleblowing»)[68].

2. Dans quelles conditions peut-on traiter ces données ?

47. Il est, en principe, interdit de traiter des données sensibles[69]. On peut tout de même traiter ces données dans certains cas bien déterminés et énumérés par la loi pour chacune des trois catégories de données sensibles[70]. Ces exceptions doivent être interprétées restrictivement[71].

48. Les principales bases de traitement sont pour ce qui concerne les données, les suivantes, reprises sous forme de synthèse :

---

67 Y. Poullet et Th. Léonard, «La protection des données à caractère personnel en pleine (r)évolution», *J.T.*, 1999, nº 42, p. 388.

68 Commission de la protection de la vie privée, «Recommandation nº 1/2006 relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel», 29 novembre 2006, p. 3, www.privacycommision.be.

69 Art. 6, 7 et 8 de la loi du 8 décembre 1992.

70 Art. 6, 7 et 8 de la loi du 8 décembre 1992.

71 C.C., 14 février 2008, arrêt nº 15/2008, point B.27, www.cass.be.

<table>
<tr><th>Données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, etc.</th><th>Données relatives à la santé</th><th>Données judiciaires</th></tr>
<tr><td colspan="2">La personne concernée a donné son consentement par écrit à un tel traitement, pour autant que ce consentement puisse à tout moment être retiré par celle-ci.</td><td></td></tr>
<tr><td colspan="2">Le traitement est nécessaire afin d'exécuter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail.</td><td></td></tr>
<tr><td colspan="2">Le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement.</td><td></td></tr>
<tr><td colspan="2">Le traitement porte sur des données manifestement rendues publiques par la personne concernée.</td><td></td></tr>
<tr><td colspan="2">Le traitement 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.</td><td></td></tr>
<tr><td colspan="2">Le traitement est nécessaire aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée et le traitement est effectué sous la surveillance d'un professionnel des soins de santé.</td><td></td></tr>
<tr><td>Le traitement des données à caractère personnel de telles données sensibles est permis par une loi, un décret ou une ordonnance pour un autre motif important d'intérêt public.</td><td>Le traitement est rendu obligatoire par ou en vertu d'une loi, d'un décret ou d'une ordonnance pour des motifs d'intérêt public importants.</td><td>Le traitement par d'autres personnes qu'une autorité publique ou un officier ministériel lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d'une loi, d'un décret ou d'une ordonnance.</td></tr>
<tr><td colspan="2">Le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.</td><td>Le traitement par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige.</td></tr>
</table>

49. À l'exception des données judiciaires, le traitement de données sensibles est permis notamment lorsque le traitement est nécessaire afin d'exécuter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, lorsque le traitement est nécessaire à des fins de médecine préventive ou

encore lorsque le traitement est réalisé avec le consentement écrit de la personne concernée. Concernant cette dernière hypothèse, le législateur interdit toutefois, à l'article 27 de l'arrêté royal du 13 février 2001, tout traitement de données sensibles sur la seule base du consentement écrit de la personne concernée 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 l'empêchant de refuser librement son consentement. Dans une telle situation, le consentement écrit permet néanmoins le traitement s'il s'agit d'octroyer un avantage à la personne concernée.

La loi du 8 décembre 1992 et son arrêté d'exécution prévoient également des modalités particulières à respecter et qui s'ajoutent à celles définies pour le traitement de données à caractère personnel non sensibles[72].

3. Quelques applications…

50. Nous nous proposons de donner un aperçu nécessairement non exhaustif de la problématique au travers d'exemples pris dans chaque catégorie de données sensibles.

a. Le traitement de données sensibles dans le cadre de la lutte contre la discrimination

51. L'employeur peut être amené à devoir traiter des données sensibles, relatives par exemple, à l'origine ethnique ou à un handicap pour se conformer à des obligations positives ou négatives mises à sa charge en matière de lutte contre la discrimination[73]. Comme le relève J. Ringelheim, l'employeur ne pourra traiter de telles données qu'en s'appuyant sur les exceptions prévues par la loi. En sus de l'hypothèse d'un consentement du travailleur, on relèvera que l'employeur peut justifier que cela est nécessaire pour se conformer à des droits et obligations spécifiques en matière du travail ou encore que ce traitement est autorisé par une loi, un décret ou une ordonnance pour des motifs d'intérêt public importants[74].

---

72 *Cf.* n° 90 et suiv., *infra*. Voy. également l'article 42, § 2, 3° de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé et qui subordonne la communication de données relatives à la santé à des tiers à condition d'une autorisation préalable du Comité sectoriel de la Sécurité Sociale et de la Santé, sauf exceptions prévues dans cette disposition.

73 Pour une application de ces principes, voy. Commission de la protection de la vie privée, Avis n° 07 relatif au projet « monitoring des 'groupes à potentiel' au sein du fichier du personnel du Ministère de la Communauté flamande géré via le système 'Vlimpers' », 22 mars 2006, www.privacycommission.be.

74 J. Ringelheim, « Recueil des données personnelles et lutte contre les discriminations. Une tension nécessaire entre non-discrimination et vie privée », *in Les nouvelles lois luttant contre la discrimination*, Die Keure / La Charte, 2008, pp.91-92. La Commission de la protection de la vie privée a déjà admis que ces deux causes d'exceptions pouvaient justifier la mise en place par la Communauté flamande d'un

b. Le traitement des données relatives à la santé des travailleurs[75]

52. Comme rappelé ci-avant, par « données relatives à la santé », on entend que les informations doivent *se rapporter* à la santé de l'individu, les données ne faisant que *révéler* l'état de santé d'un individu ne tombant pas dans la catégorie des données relatives à la santé.

> Dès lors, s'il ne fait pas de doute que l'information selon laquelle une travailleuse est enceinte ou qu'un employé est affecté d'un handicap mental ou physique peut bel et bien constituer une donnée relative à la santé, qu'en est-il de l'information selon laquelle l'employé est en incapacité de travailler sur la base d'un certificat médical ? En effet, même si le certificat ne mentionne pas la maladie ou le handicap qui frappe le travailleur, l'information semble néanmoins *se rapporter* nécessairement à l'état de santé du travailleur dès lors que l'incapacité constatée par le médecin est forcément motivée par un problème de santé. Cette interprétation pourrait être toutefois discutée au vu d'un avis de la Commission de la protection de la vie privée qui avait qualifié certaines données relatives à la santé dans le contexte de la relation de travail de « données administratives »[76].

En sus des conditions applicables à tout traitement de données à caractère personnel et à celles applicables aux données sensibles que nous aborderons ci-après, il convient de signaler deux particularités propres aux données relatives à la santé.

Tout d'abord, le traitement des données relatives à la santé peut, sauf dans le cas d'un consentement écrit de la personne concernée ou lorsque le traitement est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée, uniquement être effectué sous la responsabilité d'un professionnel des soins de santé[77]. La notion de « professionnel de la santé » n'a été définie ni dans la loi du 8 décembre 1992 ni dans un arrêté d'exécution. Selon l'exposé des motifs de la loi du 11 décembre 1998 qui a introduit cette modification dans la loi du 8 décembre 1992, ces termes renvoient « à un concept vaste qui fait référence à l'ensemble des personnes qui prestent des soins de santé à l'égard d'autres personnes dans l'exercice de leur profession »[78]. Ainsi, après avoir estimé qu'un test d'haleine implique le

---

système de monitoring des groupes à potentiels au sein de son fichier du personnel (*cf.* Commission de la protection de la vie privée, Avis 03/2004 du 15 mars 2004 et 07/2006 du 22 mars 2002 commenté par J. Ringelheim, *op. cit.*, pp. 92-94).

75 Cette section est inspirée par une partie de l'article co-rédigé par K. Rosier, S. Gilson et N. Hautenne et intitulé « Les informations médicales dans la relation de travail » (*Orientations*, n° spécial 35 ans, mars 2005, pp. 65-67).

76 *Ibidem*.

77 Art. 7, § 4, de la loi du 8 décembre 1992.

78 Exposé des motifs de la loi du 8 décembre 1992, *Doc. Parl.*, Ch. Repr., sess. ord. 1997-1998, 1566/1-n° 1, p. 39 ; Th. Léonard, « La protection des données à caractère personnel et l'entreprise », *Le guide juridique*

traitement de données de santé, le Conseil d'État a jugé que, en application de l'article 7, § 4, alinéa 1er, « de tels tests ne peuvent être réalisés que par un professionnel des soins de santé qui est tenu au secret y compris vis-à-vis de l'autorité qui est seulement autorisée à savoir si l'agent est apte ou non à exercer ses fonctions ». Dès lors que ces conditions n'avaient pas été respectées, le Conseil d'État constata l'illicéité du traitement[79].

L'intervention d'un professionnel de la santé n'est, en revanche, pas requise si le travailleur consent par écrit à ce que ce traitement ne soit pas effectué sous une telle responsabilité[80]. Il convient néanmoins de noter qu'en application de l'arrêté royal du 28 mai 2003 relatif à la surveillance de la santé des travailleurs, l'intervention du conseiller en prévention-médecin du travail est rendu obligatoire pour certains traitements de données médicales de sorte qu'il nous semble que l'employeur ne pourra se passer de l'intervention du conseiller en prévention-médecin du travail en faisant usage de l'exception du consentement.

53. Par ailleurs, les données relatives à la santé ne peuvent être collectées qu'auprès de la personne concernée[81]. Il est donc, en principe, interdit de se procurer de telles données auprès de tiers. La loi du 8 décembre 1992 n'autorise une telle collecte que lorsque le traitement est effectué dans le respect des conditions définies par la loi (en ce qui concerne la supervision par un professionnel des soins de santé) et par arrêté royal (en l'occurrence l'arrêté royal du 13 février 2001) et dans la mesure où les données relatives à la santé sont nécessaires aux fins du traitement[82] ou lorsque la personne concernée n'est pas à même de fournir les données elle-même.

---

de l'entreprise, Titre XI, Livre 112.1, 2e éd., Bruxelles, Kluwer, p. 36. La loi ne fournit pas de liste des professions médicales et paramédicales concernées. La question se pose de savoir si un psychologue peut être qualifié de professionnel des soins de santé. Preste-t-il des soins de santé ? Cette question est controversée (H. Nys, *La médecine et le droit*, Diegem, Kluwer, 1995, p. 29). Cette question peut revêtir un intérêt particulier dans l'hypothèse où des tests psychologiques devraient être mis en œuvre par l'employeur ou que l'employeur envisage d'offrir un service de soutien psychologique à ses employés par le biais d'un psychologue d'entreprise. L'intervention d'un psychologue suffirait-elle alors à remplir l'obligation de contrôle par un professionnel des soins de santé ?

79 C.E., arrêt nº 150.861 du 27 octobre 2005, cité par J.-M. Van Gyseghem et J.-Ph. Moiny, « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *R.D.T.I.*, 2009, nº 35, p. 90.

80 Exposé des motifs de la loi du 8 décembre 1992, *Doc. Parl.*, Ch. Repr., sess. ord. 1997-1998, 1566/1 nº 1, p. 38. Il est à noter qu'étonnamment le législateur n'a pas étendu les réserves énoncées à l'article 27 de l'arrêté royal du 13 février 2001 relatives à la possibilité de s'appuyer sur le consentement du travailleur pour traiter des données sensibles dans l'hypothèse où l'employeur entend se passer de l'intervention d'un professionnel des soins de santé moyennant le consentement du travailleur.

81 Art. 7, § 5 de la loi du 8 décembre 1992.

82 Ce qui devrait de toute façon toujours être le cas en vertu de l'article 4, 3° de la loi du 8 décembre 1992.

c. Le traitement des données relatives au casier judiciaire

54. Le traitement des données judiciaires est interdit, même de l'accord de la personne concernée. Un employeur ne pourra donc traiter les données judiciaires que si ce traitement est nécessaire à la gestion du contentieux de l'employeur ou lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

> Qu'en est-il dès lors de la légalité de la pratique consistant à demander à un candidat à l'embauche la production d'un « certificat de bonnes vie et mœurs » ?
>
> Il convient, tout d'abord, de constater la fin de certificat désormais remplacé par un extrait de casier judiciaire[83].
>
> Le recueil d'informations dans le cadre du recrutement et de la sélection doit se faire dans le respect de l'obligation de bonne foi tant dans le chef de l'employeur que dans celui du candidat. L'article 11 de la convention collective de travail n° 38[84] pose une première limite en matière de demande d'informations à un travailleur en stipulant que la vie privée des candidats doit être respectée lors de la procédure de sélection. Cela implique, selon cette disposition, que des questions sur la vie privée ne se justifient que si elles sont pertinentes en raison de la nature et des conditions d'exercice de la fonction. Enfreindre ce principe serait constitutif d'un manquement à l'obligation de bonne foi dans le chef de l'employeur[85]. Si la demande d'informations n'est pas justifiée, le travailleur n'est pas tenu de les donner spontanément et est même autorisé à mentir si la question lui est posée[86].
>
> Un extrait de casier judiciaire contient, par ailleurs, non seulement des données à caractère personnel ordinaires (nom, prénom, adresse,…) mais égale-

---

83 Voy. Les articles 595 et 596 C.I.C. modifiés par la loi du 31 juillet 2009 portant diverses dispositions concernant le Casier judiciaire central et arrêt de la Cour constitutionnelle du 13 janvier 2011 annullant partiellement l'article 596 C.I.C. tel que modifié (C.C., 13 janvier 2001, n° 1/2011). Suite à un arrêt du Conseil d'État ayant annulé la circulaire qui organisait la délivrance de ce certificat par les communes, la ministre de la Justice avait adopté une nouvelle circulaire le 2 février 2007 qui prévoyait la délivrance d'un « extrait de casier judiciaire » (Circulaire n° 095 du 2 février 2007 relative à la délivrance d'extrait de casier judiciaire, *M.B.*, 9 février 2007. Une proposition de loi a d'ailleurs été déposée à la chambre le 30 juillet 2007 visant à répondre aux remarques du Conseil d'État et assurer une certaine sécurité juridique en donnant une base légale aux certificats de bonne conduite, vie et mœurs [Proposition de loi relative au certificat de bonnes conduite, vie et mœurs, *Doc. parl.*, Chambre, 52 -081/001]). Cette circulaire avait elle-même été annulée par le Conseil d'État le 26 janvier 2009 (C.E., arrêt du 26 janvier 2009, n° 189.761 cité dans « Bonnes vie et mœurs : suite des errements d'un très long dossier », actualité du 3 mars 2009, http://www.uvcw.be). Voy. également sur cette question, S. Gilson, « Motif grave et bonne mœurs » *in Le congé pour motif grave*, Limal, Anthemis, 2011, pp. 334-335.

84 Convention collective de travail n° 38 du 6 décembre 1983 concernant le recrutement et la sélection de travailleurs modifiée par les conventions collectives de travail n° 38*bis* du 29 octobre 1991, n° 38*ter* du 17 juillet 1998, n° 38*quater* du 14 juillet 1999 et n° 38*quinquies* du 21 décembre 2004.

85 H. Clauwaert, « Le respect de la vie privée lors de la recherche d'un emploi et de la sélection de personnel », *Rev. trav.*, 1997, p. 13.

86 G. Demez, « Le droit au respect de la vie privée dans le cadre des tests préalables à l'embauche » *in Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. J.B.B., 2005, p. 63.

ment des données que l'on qualifie de données judiciaires au sens de l'article 8, § 1er de la loi du 8 décembre 1992, dès lors qu'elles sont relatives à des condamnations ayant trait à des infractions. En vertu de cette disposition, le traitement de ces données est, en principe, interdit sauf dans le cadre d'exceptions qui sont énumérées limitativement par l'article 8, § 2 de la loi du 8 décembre 1992.

Dès lors que le traitement de telles données n'entre pas dans le cadre de la gestion du contentieux de l'employeur, il ne reste alors que la possibilité de traiter de telles données lorsque cela est nécessaire à la réalisation de finalités qui sont fixées par ou en vertu d'une loi, d'un décret ou d'une ordonnance. La Commission de la protection de la vie privée a d'ailleurs indiqué, dans un avis qu'elle a émis le 11 février 2002[87] que « à défaut de réglementation appropriée, l'employeur ne pourra que prendre connaissance, avec le consentement de la personne concernée, du contenu du certificat, sans en prendre note, ni conserver de mention à ce sujet pour autant que comme exigé par l'article 11 de la C.C.T. nº 38, ces informations se justifient par rapport à la nature de la fonction convoitée ». Le raisonnement sous-jacent est sans doute qu'en l'absence d'inclusion de ces données dans un fichier ou de traitement automatisé sur ces données, la loi ne s'applique pas. On peut alors se demander pourquoi mentionner une exigence spécifique de consentement du travailleur, consentement qui ne permet pas, par ailleurs, de lever l'interdiction de traitement[88].

55. En ce qui concerne l'existence d'une loi permettant le traitement de données relatives à des suspicions quant à l'existence d'une infraction, la Commission de la protection de la vie privée a estimé qu'il ne pouvait s'agir que d'une loi belge.

La question a été abordée dans le cadre d'une analyse de l'admissibilité de traitements de données intervenant dans la mise en œuvre d'un système d'alerte professionnelle (auquel il est également référé par le terme « *whistleblowing* »)[89].

Ce système vise à permettre, voire à encourager, le signalement par les travailleurs d'une entreprise du comportement d'un membre de leur organisation, contraire, selon eux, à une législation ou à une réglementation ou aux règles primordiales établies par leur organisation. Le plus souvent la dénonciation se fait de manière anonyme.

La Commission identifie deux bases potentielles aux traitements intervenant dans un tel système :

---

87 Commission de la protection de la vie privée, Avis nº 08/2002 relatif aux traitements de données à caractère personnel réalisés par les sociétés privées d'intérim, 11 février 2002, p. 3, www.privacycommision.be.

88 *Cf.* nº 48, *supra*.

89 Commission de la protection de la vie privée, « Recommandation nº 1/2006 relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel », 29 novembre 2006, www.privacycommision.be.

1° l'existence d'une obligation légale ou réglementaire lui imposant de traiter des données à caractère personnel via un système d'alerte ;

2° en l'absence d'une telle obligation légale, un intérêt légitime dans son chef à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne mise en cause.

Elle estime toutefois que « dans la mesure où les données fournies et traitées sont des données à caractère personnel au sens de l'article 8 de la LVP, en l'espèce des données à caractère personnel concernant des suspicions relatives à des infractions, l'article 5 de la LVP ne suffit pas pour permettre à l'organisation de traiter les données visées »[90]. Il ne reste que la possibilité d'invoquer un fondement légal ou réglementaire pour le traitement exceptionnel de ces données tel que précisé à l'article 8, § 2 de la loi du 8 décembre 1992. La Commission estime toutefois qu'il doit s'agir d'une disposition légale du droit belge et qu'une obligation légale étrangère ne peut pas entrer en ligne de compte.

B. Les données faisant l'objet d'une règlementation particulière

56. Certaines données font l'objet d'une réglementation particulière. Nous pensons notamment aux données générées pour les besoins des communications électroniques et qui ne peuvent être traitées que pour certaines finalités par les opérateurs[91] ou seulement dans certaines conditions par tout un chacun[92].

57. Ainsi en est-il également du numéro de registre national qui, sauf autorisation octroyée par le biais d'une loi ou d'un arrêté royal ou par le comité sectoriel Registre national institué au sein de la Commission de la protection de la vie privée, ne peut être traité[93].

L'employeur peut-il demander et conserver le numéro d'identification du registre national de ses employés et dans l'affirmative, dans quel cadre ?

Le numéro d'identification du registre national est une donnée à caractère personnel qui fait l'objet d'une réglementation spécifique. La loi du 8 août 1983 organisant un registre national des personnes physiques définit les possibilités d'accès au registre national. C'est dans ce cadre que son article 8, § 2 dispose, de façon tout à fait générale, qu'il n'est pas possible de trai-

90 Commission de la protection de la vie privée, « Recommandation n° 1/2006 relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel », 29 novembre 2006, p. 3, www.privacycommision.be.

91 *Cf.* art. 122 et 123 de la loi du 13 juin 2005 sur les communications électroniques.

92 *Cf.* art. 124, 125 et 128 de la loi du 13 juin 2005.

93 *Cf.* art. 5 et 8 de la loi du 8 août 1983 organisant un registre national des personnes physiques.

ter le numéro d'identification du registre national sans y avoir été autorisé. L'article 13 de la loi prévoit par ailleurs que la violation de cette disposition est passible d'une peine d'emprisonnement de huit jours à un an et d'une amende de cent euros à deux mille euros. Ce régime est donc plus restrictif que celui prévu par la loi du 8 décembre 1992 qui a également vocation à régir le traitement de ce numéro dès lors qu'il s'agit d'une donnée à caractère personnel. L'une des implications de cette loi est que l'employeur qui traite cette donnée doit en principe[94] déclarer le traitement y afférent auprès de la Commission de la protection de la vie privée.

L'autorisation d'utiliser le numéro d'identification du registre national est octroyée par le comité sectoriel du registre national créé au sein de la Commission de la protection de la vie privée. Toutefois, ce comité n'est habilité à délivrer des autorisations qu'à certaines catégories de personnes et pour des finalités particulières. Ainsi les entreprises privées ne peuvent éventuellement bénéficier d'une autorisation que dans l'hypothèse où cette donnée s'avère nécessaire à l'accomplissement de tâches d'intérêt général qui leur sont confiées par ou en vertu d'une loi, d'un décret ou d'une ordonnance ou de tâches reconnues explicitement comme telles par le comité sectoriel précité ou encore lorsqu'elles agissent en qualité de sous-traitants des autorités publiques belges et des organismes publics ou privés de droit belge pour autant qu'eux-mêmes soient susceptibles de se voir octroyer une autorisation.

Le régime d'autorisation mis en place par la loi est donc pour le moins restrictif. Pourtant, les entreprises qui disposent de cette donnée doivent être à même de le justifier par rapport à la législation en vigueur. D'ailleurs, dans son formulaire de notification des traitements de données, la Commission de la protection de la vie privée invite à indiquer si le traitement déclaré porte sur le numéro d'identification du registre national et, dans l'affirmative, sur quelle base légale.

Le traitement du numéro d'identification du registre national se justifie toutefois au regard de certaines dispositions légales relatives à la sécurité sociale. En effet, l'employeur peut, dans certaines circonstances, être tenu de fournir cette information à l'institution chargée de la perception des cotisations de sécurité sociale, et ce en dehors du régime des autorisations. Ainsi, en vertu de l'article 4, 2° de l'arrêté royal du 5 novembre 2002 instaurant une déclaration immédiate de l'emploi, en application de l'article 38 de la loi du 26 juillet 1996 portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux des pensions, l'employeur est obligé de traiter le numéro d'identification à la sécurité sociale du travailleur. Or ce numéro correspond au numéro d'identification du registre national s'il s'agit d'un assuré social repris dans ledit registre comme il résulte de l'article 1, 4° de arrêté royal portant des mesures en vue d'instaurer une carte d'identité sociale à l'usage de tous les assurés sociaux, en application des articles 38, 40, 41 et 49 de la loi

[94] Voyez cependant les exceptions à l'obligation de déclaration pour les traitements relatifs à l'administration des salaires et à la gestion du personnel (A.R. du 13 février 2001, art. 51 et 52).

du 26 juillet 1996 portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux des pensions.

En dehors de ce cadre d'utilisation, l'employeur doit donc veiller à ne pas recueillir ni conserver le numéro d'identification du registre national à moins qu'il puisse se fonder sur une loi ou une autorisation *ad hoc*.

Section 3
Les obstacles liés aux opérations de traitement envisagées

A. L'interdiction des décisions automatisées

58. La loi du 8 décembre 1992 interdit qu'une décision affectant une personne de manière significative soit prise sur le seul fondement d'un traitement automatisé de données destinées à évaluer certains aspects de sa personnalité.

Doit, par exemple, être considéré comme un traitement automatisé, la correction d'un examen à choix multiples par une machine (par exemple, dans le cadre d'un concours d'entrée dans la fonction publique).

Toutefois, cette interdiction ne s'applique pas lorsque la décision est prise dans le cadre d'un contrat ou est fondée sur une disposition légale ou réglementaire. Le contrat ou la disposition en question doivent contenir des mesures garantissant la sauvegarde des intérêts de l'intéressé. À tout le moins, celui-ci doit avoir le droit de faire valoir *utilement* son point de vue.

B. La problématique des transferts de données hors du territoire de l'E.E.E.

59. Parmi les opérations de traitement qui peuvent être effectuées, il en est une qui est réglementée de manière particulière : il s'agit du transfert de données vers un territoire situé hors de l'Espace économique européen.

La notion de transfert n'est définie ni dans la directive 95/46/CE, ni par la loi du 8 décembre 1992. Intuitivement, on serait tenté de penser que le transfert implique l'envoi des données et est distinct de la simple possibilité de permettre la consultation de celles-ci. Des discussions se sont toutefois élevées sur la question de savoir si la diffusion d'informations sur internet correspond à un transfert dès lors que les données sont de fait accessibles à toute personne qui accède au site, sans toutefois qu'une réponse claire à ce sujet n'émerge.

La C.J.C.E. a, dans l'arrêt *Lindqvist* du 6 novembre 2003, décidé qu'une personne mettant en ligne des informations sur un site hébergé par un tiers

n'opérait pas de transfert de données vers des pays tiers[95]. La Cour a notamment estimé que « Eu égard, d'une part, à l'état du développement d'internet à l'époque de l'élaboration de la directive 95/46 et, d'autre part, à l'absence, dans son Chapitre IV, de critères applicables à l'utilisation d'internet, on ne saurait présumer que le législateur communautaire avait l'intention d'inclure prospectivement dans la notion de « transfert vers un pays tiers de données » l'inscription, par une personne se trouvant dans la situation de M^me^ Lindqvist, de données sur une page internet, même si celles-ci sont ainsi rendues accessibles aux personnes de pays tiers possédant les moyens techniques d'y accéder »[96].

À propos de la situation de M^me^ Lindqvist, la Cour avait relevé que « Il ressort du dossier que, pour obtenir les informations figurant sur les pages internet dans lesquelles M^me^ Lindqvist avait inséré des données relatives à ses collègues, un utilisateur d'internet devait non seulement se connecter à celui-ci mais aussi effectuer, par une démarche personnelle, les actions nécessaires pour consulter lesdites pages. En d'autres termes, les pages internet de M^me^ Lindqvist ne comportaient pas les mécanismes techniques qui auraient permis l'envoi automatique de ces informations à des personnes qui n'avaient pas délibérément cherché à accéder à ces pages »[97] Le raisonnement semble reposer sur l'idée que les opérations effectuées par M^me^ Lindqvist (communiquer des informations à un hébergeur pour qu'elles figurent sur un site internet) ne constituent pas « en elles-mêmes » un « transfert vers un pays tiers de données » au motif que les données n'ont pas été transférées directement entre M^me^ Lindqvist et un internaute mais « au travers de l'infrastructure informatique du fournisseur de services d'hébergement où la page est stockée »[98]. Le raisonnement de la Cour nous semble quelque peu obscur et ne permet pas de conclure que toute mise en ligne de données ne doit pas être considérée comme un transfert[99].

60. Une réponse plus tranchée a été donnée par le Groupe de l'Article 29 dans un autre cas de figure. Lorsque la consultation est couplée à l'extraction de données contenues dans une banque de données, le Groupe de l'Article 29 a considéré qu'il ne s'agissait pas d'appliquer les règles propres au transfert

---

95 Arrêt de la C.J.C.E. 101/01 (dit arrêt *Bodil Lindqvist*), 6 novembre 2003, *R.D.T.I.*, 2004, nº 19, p. 67, note C. DE TERWANGNE.

96 Arrêt de la C.J.C.E. 101/01 (dit arrêt *Bodil Lindqvist*), 6 novembre 2003, *R.D.T.I.*, 2004, nº 67, p. 75, note C. DE TERWANGNE.

97 Arrêt de la C.J.C.E. 101/01 (dit arrêt *Bodil Lindqvist*), 6 novembre 2003, *R.D.T.I.*, 2004, nº 60, p. 74, note C. DE TERWANGNE.

98 Arrêt de la C.J.C.E. 101/01 (dit arrêt *Bodil Lindqvist*), 6 novembre 2003, *R.D.T.I.*, 2004, nº 61, p. 74, note C. DE TERWANGNE.

99 La conclusion de la Cour n'est pas partagée par tous. Voy. pour une critique de cette décision : C. DE TERWANGNE, « Affaire *Lindqvist* ou quand la Cour de justice des Communautés européennes prend position en matière de protection de données à caractère personnel », Obs. sous C.J.C.E., 6 novembre 2003, *R.D.T.I.*, 2004, pp. 90 et s.

de données. Pour le Groupe de l'Article 29[100], le fait de permettre l'accès à une banque de données depuis des pays n'offrant pas de protection adéquate implique l'utilisation de moyens localisés sur le territoire européen et a pour conséquence que toute la législation de la protection des données à caractère personnel découlant de la directive 95/46/CE est applicable à la personne qui importe les données[101].

1. Le principe de l'interdiction de transfert vers un État n'offrant pas un niveau adéquat de protection

61. Les transferts de données à caractère personnel entre pays membres de l'Union européenne et au sein de l'Espace économique européen sont libres. Une personne établie en Belgique peut donc envoyer des données à caractère personnel dans un autre pays de l'Espace économique européen[102] si cet envoi est légitime aux yeux de la loi belge, c'est-à-dire si cet envoi s'impose pour réaliser le but annoncé du traitement des données ou s'il est compatible avec ce but.

Par exemple, une entreprise belge peut envoyer les données relatives à des employés qui occupent un poste au sein d'une autre société du groupe située dans un autre État membre de l'Union européenne[103].

En revanche, on ne peut transférer des données à caractère personnel vers des pays situés en dehors de l'Espace économique européen à moins que ceux-ci n'assurent une protection des données adéquate au regard de celle assurée sur le territoire de l'Union européenne. En l'absence d'une telle règle, la forte protection garantie à l'intérieur de l'Union européenne serait rapidement vide de sens étant donné la facilité de circulation des données grâce aux nouvelles technologies.

Le transfert de données à caractère personnel faisant l'objet d'un traitement, après leur transfert vers un pays situé hors de l'Espace économique

---

100 Groupe de l'Article 29, Avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis, WP66, 27 octobre 2002, p. 7, http://ec.europa.eu/justice/policies/privacy.

101 Voy. nº 31 et suiv., *supra*.

102 Le principe de libre circulation des données au sein de l'U.E. a en effet étendu à l'E.E.E. qui inclut la Norvège, Liechtenstein et l'Islande.

103 Sur la problématique des transferts de données (documents et courriers électroniques) hors E.E.E. (en particulier vers les États -Unis) dans le cadre de procédures civiles, voy. Groupe de l'Article 29, « Document de travail 1/2009 sur la procédure d'échange d'informations avant le procès (« pre-trial discovery ») dans le cadre de procédures civiles transfrontalières », WP 158, 11 février 2009, http://ec.europa.eu/justice/policies/privacy/workinggroup.

européen, ne peut donc avoir lieu que si le pays en question assure un niveau de protection adéquat[104].

Tout responsable de traitement qui souhaite exporter des données à caractère personnel hors de l'Espace économique européen doit d'abord se demander si le pays destinataire assure un *niveau de protection adéquat* pour de telles données c'est-à-dire si le tiers à qui on communique les données est soumis au respect de principes de protection qui assurent une protection équivalente à celle qui prévaut sur le territoire européen.

Pour évaluer la qualité de la protection offerte, il faut tenir compte de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts de données, notamment de la nature des données, de la finalité et de la durée du ou des traitements envisagés ainsi que des règles de droit, générales et sectorielles, en vigueur dans le pays en cause, tout comme des règles professionnelles et des mesures de sécurité qui y sont respectées. En cas de doute, on peut s'adresser à la Commission de la protection de la vie privée pour savoir si un pays particulier offre une protection adéquate et si les transferts de données vers ce pays sont autorisés. Le Roi peut, après avis de la Commission de la protection de la vie privée, établir une « liste noire » de pays vers lesquels les données ne peuvent être envoyées[105]. Il est à noter que la Commission européenne a adopté différentes décisions constatant que certains pays offrent un niveau de protection adéquat[106].

2. Dérogations

62. Le transfert de données vers des pays qui n'offrent *pas un niveau de protection adéquat* peut néanmoins être réalisé soit dans les hypothèses où la loi le prévoit (a), soit moyennant la réunion de garanties qui pallient l'absence de protection suffisante (b).

104 Art. 21, § 1 de la loi du 8 décembre 1992.

105 Art. 21, §2 de la loi du 8 décembre 1992. Une telle liste n'existe pas à ce jour.

106 À l'heure actuelle il existe des décisions concernant la Suisse, le Canada, l'Argentine, Guernesey, les îles Féroé, l'Ile de Man, Andorre, Israël, les principes de la « sphère de sécurité » publiés par le ministère du Commerce des États-Unis d'Amérique et les données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis. Consultez à cet égard le site de la Commission européenne : http://ec.europa.eu/justice/policies/privacy/thridcountries.

a. Hypothèses dans lesquelles le transfert est permis sans obligation d'offrir des garanties complémentaires

63. Le transfert des données vers des pays qui n'offrent *pas un niveau de protection adéquat* est autorisé dans certaines hypothèses limitativement énumérées par l'article 22, § 1er de la loi du 8 décembre 1992.

C'est notamment le cas si les personnes concernées donnent leur consentement indubitable au transfert de leurs données vers un tel pays, ou lorsque le transfert est nécessaire pour exécuter un contrat avec la personne concernée, ou encore lorsque les données proviennent d'un registre public destiné à l'information du public (annuaire téléphonique, registre du commerce, par exemple) [107].

b. Hypothèses dans lesquelles le transfert est permis moyennant l'octroi de garanties complémentaires

64. Le responsable du traitement peut également offrir lui-même, par la voie contractuelle, une protection appropriée. La protection peut ainsi être assurée au moyen d'un contrat liant celui qui envoie les données et celui qui les reçoit et contenant des garanties suffisantes au regard de la protection des données. Deux modèles de contrat offrant des garanties suffisantes sont proposés par la Commission européenne [108] : l'un concerne un transfert de responsable de traitement vers un responsable de traitement [109], le second un transfert d'un responsable de traitement vers un sous-traitant [110].

65. Enfin, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays hors Espace économique européen et n'assurant pas un niveau de protection adéquat, peut être spécifiquement autorisé par arrêté royal après avis de la Commission de la protection de la vie privée, et ce lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondant [111].

---

107 Art. 22, § 2 de la loi du 8 décembre 1992.

108 Ces contrats standards sont disponibles sur le site de la Commission européenne : http://ec.europa.eu/justice/policies/privacy/modelcontracts.

109 Voy. Décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers telle que modifiée par la décision 2004/915.CE.

110 Voy. Décision de la Commission du 5 février 2010 (C(2010)593 final) relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil ; Décision 2002/16/CE relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE. Pour la notion de sous-traitant, voyez nº 84 et s., *infra*.

111 Art. 22 de la loi du 8 décembre 1992. Pour un cas d'application, voy. Commission de la protection de la vie privée, Avis nº 13/2007 relatif à un projet d'arrêté royal autorisant les transferts vers un pays non-

66. Cette autorisation *ad hoc* était prévue à l'article 26, § 2 de la directive 95/46/CE. C'est en s'appuyant sur cette même base juridique que le Groupe de l'Article 29 œuvre depuis plusieurs années, pour faciliter la vie des groupes de sociétés qui, opérant des traitements de données dans différents États membres, souhaitent obtenir des autorisations pour exporter leurs données. Dans un document de travail du 3 juin 2003, le Groupe entamait une réflexion sur la possibilité de travailler autour des règles d'entreprise contraignantes (REC) applicables aux transferts internationaux de données[112]. Dès lors qu'un groupe de sociétés aura établi un corps de règles contraignantes pour toutes les sociétés du groupe se transmettant des données et qui permettra de garantir un niveau de protection suffisant et d'assurer le respect des droits des personnes concernées par les données, il est envisageable d'introduire une demande d'autorisation dans un État membre et d'obtenir presque automatiquement par la suite les autorisations des autres États membres concernés.

> Le Groupe de l'Article 29 a procédé en plusieurs étapes. Dans le document de travail précité, il énonce les principes auxquels devraient satisfaire les REC. Dans un document adopté le 14 avril 2005, le Groupe de l'Article 29 s'est attelé à définir plus particulièrement les critères qui devaient présider au choix de l'autorité de contrôle à qui serait demandée l'autorisation de principe[113]. Par la suite, le Groupe de l'Article 29 a élaboré un document standard pour une demande d'autorisation qui devrait grandement faciliter la vie des entreprises qui font le choix de cette option[114]. Enfin, le Groupe de l'Article 29 a publié le 1er octobre 2008 un nouveau document comprenant des réponses aux questions fréquemment posées lors des demandes d'approbation des règles d'entreprise contraignantes[115]. Ces « FAQ » ont pour but d'aider les demandeurs à obtenir l'approbation de leurs règles d'entreprise contraignantes en clarifiant certaines exigences énoncées précédemment par

membre de la communauté européenne et n'assurant pas un niveau de protection adéquat de données à caractère personnel d'employés de la société General Electric, 21 mars 2007, www.privacycommission.be.

112 Groupe de l'Article 29, « Document de travail : Transferts de données personnelles vers des pays tiers : Application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données », 3 juin 2003, WP 74, disponible sur http://ec.europa.eu/justice_home/fsj/privacy.

113 Groupe de l'Article 29, « Document de travail relatif à une procédure de coopération en vue de l'émission d'avis communs sur le caractère adéquat de la protection offerte par les "règles d'entreprise contraignantes" », 14 avril 2005, WP 107 disponible sur http://ec.europa.eu/justice/policies/privacy.

114 Groupe de l'Article 29, « Recommandation 1/2007 sur une demande standard pour l'approbation de Règles d'Entreprise Contraignantes pour le transfert de données à caractère personnel », 10 janvier 2007, WP 133, disponible sur http://ec.europa.eu/justice/policies/privacy.

115 Groupe de l'Article 29, « Document de travail sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes du 24 juin 2008 », 1er octobre 2008, WP 155, http://ec.europa.eu/justice/policies/privacy.

le Groupe[116]. Elles ne sont pas exhaustives et le Groupe de l'Article 29 entend publier des mises à jour, le cas échéant.

Le document publié contient des précisions quant à la question de savoir si les REC doivent s'appliquer à toutes les données à caractère personnel traitées par le groupe de sociétés et aux sous-traitants des sociétés du groupe. Il aborde également la question de la désignation de la société responsable en cas de violation des règles d'entreprise contraignantes commise en dehors de l'Union européenne et décrit quelles sont les exigences à rencontrer en matière de consécration du droit de plainte des personnes concernées et de transparence vis-à-vis des personnes concernées. Enfin, le Groupe de l'Article 29 se penche également sur la manière dont les finalités de traitement doivent être décrites et recommande que ces REC soient énoncées au sein d'un même document.

Malgré cette louable initiative, il demeure toutefois quelques difficultés que les REC ne permettront pas d'éradiquer. La première consiste en une limite posée à la possibilité de définir des règles uniformément applicables au sein des entreprises liées par les REC. En effet, chaque entreprise sera tenue de respecter, outre les REC, le droit national applicable au traitement de données qu'il met en œuvre. Or, malgré l'objectif d'harmonisation poursuivi en la matière par la directive 95/46/CE, il a été constaté qu'il subsistait encore d'innombrables disparités entre les législations des États membres[117]. La seconde difficulté est propre à la Belgique. L'autorisation de transfert de données est, comme précisée ci-avant, obtenue par arrêté royal après avis de la Commission de la protection de la vie privée[118]. Autant dire que cela peut décourager plus d'une entreprise…

ÉTAPE 3
Affiner le projet de traitement de données au regard des exigences de la loi

67. Lorsque, au terme d'une analyse, des éventuels obstacles à la mise en œuvre du traitement de données envisagé, il apparaît que ceux-ci sont inexistants ou que le projet peut être adapté pour lever ces obstacles, il convient alors de tenir compte des exigences légales pour déterminer quelles données feront l'objet du traitement (section 1), pour assurer la transparence du traitement (section 2) ainsi que la sécurité et la confidentialité des données (section 3). Par

116 Si cet effort de clarification tend à faciliter la vie des groupes internationaux, on déplorera qu'en Belgique la procédure d'approbation des REC reste très lourde puisqu'elle requiert une approbation par arrêté royal pris après avis de la Commission de la protection de la vie privée.

117 Voy. à cet égard le Rapport de la Commission « Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE) », COM/2003/0265 final, http://eur-lex.europa.eu.

118 Art. 22 de la loi du 8 décembre 1992.

ailleurs, dans l'hypothèse où des données sensibles font l'objet du traitement, certaines exigences complémentaires doivent être rencontrées (section 4).

Section 1
Exigences quant aux données traitées

A. L'origine de données

68. L'article 4, §1er, 1° de loi du 8 décembre 1992 exige que le traitement soit licite. Le traitement doit être conforme aux lois et réglementations en vigueur, en ce compris les dispositions de la loi du 8 décembre 1992 et de l'arrêté royal du 13 février 2001. Cela implique notamment que le traitement ne peut porter sur des données qui ont été obtenues en violation d'une loi.

> Ainsi, un traitement consistant à récolter des preuves en vue de licencier un travailleur pour motif grave ne peut impliquer la violation du secret professionnel ou du secret des communications électroniques. Nous vous renvoyons à cet égard à la contribution consacrée à la problématique du contrôle des travailleurs[119].

B. Pertinence des données traitées

69. Le responsable du traitement ne peut collecter et traiter ensuite que les données qui sont *adéquates, pertinentes et non excessives* au vu des finalités annoncées. Autrement dit, il ne peut engranger des données dont il sait qu'elles ne sont pas pertinentes *et* nécessaires pour réaliser les finalités annoncées.

> Dans le processus de recrutement du personnel, l'employeur est tenu d'en respecter les limites[120] et de se plier à toutes les conditions applicables au traitement, notamment, le devoir d'information de la personne concernée.
>
> À titre d'exemple, la Commission de la protection de la vie privée a souligné, en se référant à l'article 11 de la convention collective de travail nº 38, que la loi du 8 décembre 1992 relative à la protection de la vie privée adopte les mêmes limitations à cet égard et ne permet pas que des données excessives soient récoltées, conservées, transmises,... en fin de compte, traitées. De ce fait, la Commission recommande de ne poser aucune question au candidat relative à son état de santé lorsque l'exercice de la fonction à pourvoir n'en-

---

119 Voy. au sein du présent ouvrage la contribution de R. Robert et K. Rosier consacrée à la réglementation et au contrôle de l'utilisation des technologies de la communication et de l'information sur le lieu du travail.

120 Signalons également que le Conseil de l'Europe a adopté une recommandation nº R(89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi. L'article 10 de la recommandation contient des directives particulières quant au traitement de données sensibles dans la phase de recrutement.

gendre pas de risques particuliers et de se limiter aux questions objectivement nécessaires[121].

La loi du 28 janvier 2003 relative aux examens médicaux dans le cadre des relations de travail définit les principes généraux qui s'imposent lorsque l'employeur envisage de faire passer des examens médicaux à un travailleur ou à un candidat à l'embauche ou de collecter des informations relatives à son état de santé. L'article 6 de la loi précise expressément que l'article 7 de la loi du 8 décembre 1992 sur la protection de la vie privée, portant sur les données relatives à la santé, est applicable aux informations recueillies dans le cadre d'examens médicaux. Aux termes de l'article 3 de cette loi, les tests biologiques, examens médicaux ou les collectes d'informations orales, en vue d'obtenir des informations médicales sur l'état de santé ou des informations sur l'hérédité d'un travailleur ou d'un candidat travailleur, ne peuvent être effectués pour d'autres considérations que celles tirées de ses aptitudes actuelles et des caractéristiques spécifiques du poste à pourvoir. L'examen génétique prévisionnel et le test de dépistage de l'infection par le virus de l'immunodéficience humaine sont, quant à eux, interdits.

C. Durée de conservation limitée des données

70. Le corollaire de l'exigence d'adéquation des données est que, dès que les données ne sont plus nécessaires ou pertinentes pour la finalité annoncée, le responsable du traitement doit les effacer ou les rendre anonymes[122].

Ainsi, la durée de conservation de certaines données dans la relation de travail pourra se justifier au regard, et dans les limites, de la réglementation sur les documents sociaux. L'arrêté royal nº 5 du 23 octobre 1978 relatif à la tenue des documents sociaux impose un certain nombre d'obligations aux employeurs, ainsi qu'aux personnes qui y sont assimilées[123].

Les documents sociaux dont la tenue est prescrite par l'A.R. nº 5 sont le registre général, le registre spécial du personnel, le compte individuel, le registre de présence, le contrat d'occupation d'étudiant, le contrat d'occupation de travailleur à domicile et la convention d'immersion professionnelle[124].

---

121 Commission de la protection de la vie privée, Avis d'initiative nº 08/2002 relatif au traitement de données à caractère personnel réalisé par des sociétés privées d'intérim, p. 2, www.privacycommission.be.

122 *Cf.* Art. 4, § 1, 5° de la loi du 8 décembre 1992. Il existe cependant une exception à ce principe : le responsable du traitement peut conserver des données au-delà de ce qui est nécessaire à la réalisation des finalités initiales pour autant que cette conservation soit justifiée par des fins scientifiques, statistiques ou historiques et que le responsable du traitement se plie aux exigences de l'arrêté royal du 13 février 2001.

123 L'article 1er de l'A.R. nº 5 n'est néanmoins pas applicable aux travailleurs régis par un statut qui sont occupés par l'État, les Provinces, l'Agglomération, les Fédérations de communes et les Communes (art. 3 de l'A.R. du nº 5).

124 *Cf.* Chapitre II de l'A.R. nº 5.

D. Exactitude des données conservées

71. Enfin, il faut que les données traitées soient exactes et complètes au regard des finalités poursuivies. Le responsable doit prendre toutes les mesures raisonnables pour que les données soient mises à jour et pour qu'elles le restent[125].

> Par exemple, si l'entreprise maintient des banques de données relatives aux travailleurs en service dans l'entreprise, elle a l'obligation de prendre des mesures pour s'assurer que les données enregistrées sont maintenues à jour. Cela implique, par exemple, qu'en cas de changement d'adresse d'un travailleur, elle fasse en sorte d'en être informée.

Si le principe nous semble pertinent, il est à noter que bon nombre de données ne peuvent à notre sens être qualifiées d'exactes ou inexactes dans la mesure où elles comportent par leur nature même une part de subjectivité. Les appréciations relatives à la qualité du travail d'un employé peuvent évidemment refléter en partie l'opinion d'un supérieur hiérarchique qui juge que ledit employé résiste ou non au stress, fait preuve d'efficacité et d'initiative. Cette atténuation du principe n'interdit pas que des précautions ne soient prises pour satisfaire à une exigence d'objectivité dans la mesure du possible.

> C'est ainsi que, à propos de tests de personnalité ou psychotechniques dans le cadre de recrutement, la Commission de la protection de la vie privée indique que, afin de satisfaire à l'exigence d'exactitude des données traitées, il est nécessaire que ces tests et leur interprétation soient réalisés sous la responsabilité d'un psychologue ou, et dans ce cas avec l'accord du candidat, par une personne dûment formée à ce type de missions par un psychologue[126].

Section 2
Exigences relatives à la transparence du traitement

72. Le traitement doit être loyal par rapport aux personnes concernées. Cela implique que celles-ci soient informées des traitements qui les concernent.

Il s'agit, d'une part, de fournir une information individuelle aux personnes concernées par le traitement et, d'autre part, de déclarer le traitement au moyen d'un formulaire *ad hoc* auprès de la Commission de la protection de la vie privée. La déclaration de traitement est ainsi intégrée dans un registre public accessible à tous et, depuis quelques années, consultable sur internet.

---

125 Art. 4, § 1, 4° de la loi du 8 décembre 1992. L'article 16, §2, 1° de la loi du 8 décembre 1992 impose au responsable de traitement de faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des articles 4 à 8 de la loi du 8 décembre 1992.

126 Commission de la protection de la vie privée, Avis d'initiative n° 08/2002 relatif au traitement de données à caractère personnel réalisé par des sociétés privées d'intérim, p. 4, www.privacycommission.be.

Si ces deux exigences procèdent du même but, à savoir assurer une transparence des traitements effectués, tant le contenu que la forme et le moment de l'information diffèrent.

Tandis que la déclaration prend la forme d'un formulaire avec cases à remplir par référence à différents lexiques sur les finalités et types de données traitées, la communication de l'information individuelle est moins encadrée.

A. Déclaration à la Commission de la protection de la vie privée

73. La déclaration doit être préalable à la mise en œuvre du traitement[127]. Cette déclaration se fait auprès de la Commission de la protection de la vie privée au moyen d'un formulaire type (sur papier ou en ligne). Une contribution financière est à verser à chaque déclaration.

Tous les renseignements transmis dans la déclaration sont repris dans un registre public. Ce registre peut être librement consulté par quiconque sur place, dans les locaux de la Commission de la protection de la vie privée ou en ligne.

1. Contenu de la déclaration

74. La déclaration comporte une description des caractéristiques du traitement. Doivent y figurer, notamment[128] :

- les finalités du traitement ;
- les catégories de données traitées (pas les données elles-mêmes) ;
- les catégories de destinataires à qui les données peuvent être fournies ;
- les garanties entourant la communication de données à des tiers ;
- les moyens par lesquels les personnes à propos desquelles des données sont traitées en seront informées ;
- les mesures prises pour faciliter l'exercice du droit d'accès ;
- les catégories de données destinées à être transmises à l'étranger et les pays de destination ;
- la période au-delà de laquelle les données ne peuvent plus être gardées, utilisées ou diffusées.

75. Par ailleurs, aux termes de l'article 25 de l'arrêté royal du 13 février 2001, le responsable de traitement doit indiquer soit lors de l'information, soit dans la déclaration à la Commission de la protection de la vie privée, la base légale

127 Art. 17 de la loi du 8 décembre 1992.

128 Art. 17, § 2 de la loi du 8 décembre 1992.

(article de la loi) sur laquelle il se fonde pour traiter les données sensibles[129]. En réalité, le formulaire de déclaration de traitement comporte un champ au sein duquel cette mention est automatiquement requise lorsque le responsable de traitement déclare par ailleurs traiter des données sensibles. En pratique, le responsable de traitement mentionnera donc la base légale au sein de la déclaration de traitement, à moins qu'il ne soit dispensé de cette déclaration en vertu des exceptions prévues en ce sens.

2. Exceptions à l'obligation de déclaration

76. Outre le fait qu'il ne faut pas déclarer les traitements manuels (sur papier ou microfiches), une série de traitements automatisés de données font l'objet d'une dispense de déclaration[130]. Il s'agit notamment, dans les limites admises par l'arrêté royal du 13 février 2001[131], des traitements réalisés par l'administration des salaires du personnel travaillant pour le responsable du traitement et des traitements pour l'administration du personnel au service du responsable du traitement. Ces exceptions sont également reprises dans le formulaire de déclaration proposé par la Commission de la protection de la vie privée.

Il convient de bien vérifier pour chaque exception dans quelle limite celle-ci est valable. Ainsi, l'exception prévue à l'article 52 de l'arrêté royal pour les traitements de données à caractère personnel qui visent exclusivement l'administration du personnel au service du ou travaillant pour le responsable du traitement ne joue pas si le traitement se rapporte à des données relatives à la santé de la personne concernée, à des données sensibles ou judiciaires au sens des articles 6 et 8 de la loi ou à des données destinées à une évaluation de la personne concernée.

Le défaut de déclaration est sanctionné pénalement[132].

Si le responsable de ces traitements est dispensé de la formalité de déclaration, il doit tout de même tenir à la disposition de toute personne qui en fait la demande les mêmes renseignements que ceux contenus dans la déclaration[133]. Cet exercice n'est certes pas vain : il contribue à une bonne gestion interne des ressources informationnelles.

---

129 Art. 25, 4 de la loi du 8 décembre 1992.

130 Ces exceptions sont prévues aux articles 51 à 62 de l'A.R. du 13 février 2001. Il convient de bien vérifier pour chaque exception dans quelle limite celle-ci est valable. Ces exceptions sont également reprises dans le formulaire de déclaration proposé par la Commission de la Protection de la Vie Privée.

131 Pour une description synthétique des cas d'exemptions et des conditions y relatives, voyez http://www.privacycommission.be/declarations/lexique1.htm, question 2.13.

132 Art. 39, 7° de la loi du 8 décembre 1992.

133 Voy. plus particulièrement : art. 51 et 52 de l'A.R. du 13 février 2001.

77. Il est encore à noter que le responsable du traitement doit également informer la Commission de la protection de la vie privée de la suppression d'un traitement automatisé ou de toute modification de traitement intervenant postérieurement à la déclaration[134].

B. Information des personnes concernées

1. Quand l'information doit-elle être donnée ?

78. Il convient de distinguer deux hypothèses : celle où le responsable du traitement collecte les données directement auprès de la personne concernée[135] de celle où les données ne lui sont fournies par elle[136].

Dans le premier cas de figure, le responsable du traitement doit fournir l'information requise au plus tard au moment de la collecte, à moins que ces personnes n'aient déjà reçu lesdites informations auparavant.

Il se peut également que le responsable du traitement obtienne les données, non auprès de la personne concernée, mais auprès d'un tiers par exemple. Dans ce cas, le responsable du traitement doit informer les personnes concernées, à moins qu'elles ne le soient déjà, au moment de l'enregistrement des données ou, au plus tard, lors de la première communication à un tiers si une telle communication est envisagée.

2. Quelle est l'information à fournir ?

79. La principale difficulté dans le cadre de l'information individuelle est de fournir une information suffisamment précise au regard de la loi tout en étant toutefois suffisamment large que pour comprendre l'ensemble des opérations qui seront nécessaires au traitement.

En effet, la loi prévoit que l'information doit *au minimum* porter sur les points suivants :

- le nom et l'adresse du responsable du traitement ;
- les finalités de traitement ;
- si les données seront traitées à des fins de marketing direct (toutes démarches de promotion), l'existence d'un droit de s'opposer gratuitement à un tel traitement[137].

---

134 Art. 17, § 7 de la loi du 8 décembre 1992. Pour en savoir plus sur la fin des traitements, voyez http://www.privacycommission.be/declarations/lexique1.htm, questions 2.19 et 2.20.

135 Art. 9, § 1 de la loi du 8 décembre 1992.

136 Art. 9, § 2 de la loi du 8 décembre 1992.

137 Non seulement la loi du 8 décembre 1992 impose d'annoncer l'existence d'un droit d'opposition, mais l'arrêté royal en son article 34 impose au responsable du traitement de proposer à la personne concernée d'exercer son droit d'opposition.

La loi impose toutefois au responsable du traitement de fournir toute autre information supplémentaire qui permet d'assurer un traitement loyal des données au vu des circonstances particulières de traitement et notamment :

– les destinataires ou les catégories de destinataires des données (personnes à qui les données seront communiquées) ;
– le caractère obligatoire ou non de la réponse, ainsi que les conséquences éventuelles d'un défaut de réponse ;
– l'existence pour chacun d'un droit d'accès aux données qui le concernent et d'un droit de rectification de celles-ci.

Cette liste n'est donc pas exhaustive et il convient de déterminer au cas par cas quelle information devrait être donnée pour assurer un traitement loyal.

> Ainsi, la Commission de la protection de la vie privée préconise-t-elle lors de la mise en place d'un système d'accès fonctionnant grâce à des données biométriques (images, empreintes digitales, etc.) que les personnes reçoivent, outre les informations minimales prévues par la loi, une information à propos du type de système biométrique utilisé (type de stockage notamment), de l'existence d'un taux d'erreur de reconnaissance inhérent à tout système biométrique et de la procédure à suivre par la personne concernée lors d'une prétendue non-reconnaissance par le système[138].

3. Comment l'information doit-elle être fournie ?

80. Si l'information ne doit pas nécessairement être donnée par écrit, on ne peut que le conseiller à des fins probatoires. Il est donc recommandé de faire figurer dans un document remis au travailleur soit lors de l'engagement (contrat de travail ou règlement de travail, par exemple), soit sur le document lui demandant de fournir certaines informations, une clause l'informant des traitements de données qui seront effectués sur les informations que le travailleur fournit ou que l'employeur sera amené à recevoir de tiers[139].

4. Existe-t-il des exceptions à l'obligation d'information ?

81. Lors d'une collecte auprès de tiers, le responsable du traitement est, toujours, *dispensé de l'obligation* d'information dans deux hypothèses.

---

138 Commission de la protection de la vie privée, Avis d'initiative n° 17/2008 relatif aux traitements de données biométriques dans le cadre de l'authentification de personnes (A/2008/017), 9 avril 2008, p. 18, www.privacycommission.be.

139 Pour la fourniture d'informations par le biais de communications électroniques, voy. Groupe de l'Article 29, Avis 10/2004 sur « Dispositions davantage harmonisées en matière d'informations », WP100, 25 novembre 2004, p. 7, http://ec.europa.eu/justice_home/fsj/privacy.

82. La première concerne le cas de figure où la démarche d'information s'avère impossible ou extrêmement difficile[140].

> La loi ne précise pas ce qui pourrait constituer un obstacle rendant impossible ou extrêmement difficile l'information. On peut aisément concevoir des difficultés matérielles : le nombre de personnes concernées, le fait que l'on ne soit pas en mesure de les contacter, etc. Rien n'exclut de pouvoir également concevoir des impossibilités d'une autre nature. Ainsi, confrontée à la question de l'information à fournir par un avocat aux personnes à propos desquelles il a obtenu des informations, C. de Terwangne indique que l'exception peut aussi se concevoir en raison d'une impossibilité fonctionnelle (dans le sens où l'information contrarierait l'œuvre de l'avocat) ou légale (dans la mesure où il existe une obligation légale de respecter le secret professionnel)[141]. Dans le droit fil de ce raisonnement, il nous semble que, dans certaines hypothèses, on pourrait invoquer une impossibilité d'informer lorsque cette démarche irait à l'encontre de l'exercice des droits de défense ou de la gestion d'un contentieux impliquant un ou plusieurs membres du personnel.

Celui qui invoque l'impossibilité ou les efforts disproportionnés qu'impliquerait pour lui le fait d'informer les personnes concernées doit se justifier auprès de la Commission de la protection de la vie privée. Il rajoute cette justification dans la déclaration qu'il doit faire avant de démarrer son traitement[142].

83. Une seconde exception est prévue : le responsable du traitement est exempté de l'obligation d'information 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[143]. La loi du 8 décembre 1992 ne semble donc pas exiger que la loi, le décret ou l'ordonnance en question prévoie la communication ou l'enregistrement en tant que tels. À lire la loi du 8 décembre 1992, il suffit que cet enregistrement soit effectué pour l'application de dispositions légales.

Toutefois si une prise de contact s'établit (plus tard) avec une ou plusieurs personnes concernées, le responsable du traitement devra à ce moment fournir les informations énumérées[144].

---

140 Art. 9, § 2, e) de la loi du 8 décembre 1992.

141 C. de Terwangne, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *in Cabinets d'avocats et technologies de l'information : balises et enjeux*, Bruxelles, Bruylant, 2005, p. 171.

142 Art. 31 de l'A.R. du 13 février 2001.

143 Art. 9, § 2, e) de la loi du 8 décembre 1992.

144 Art. 30 de l'A.R. du 13 février 2001.

Section 3
Exigences relatives à la sécurité et à la confidentialité des données

A. Veiller à la confidentialité des données

84. Le responsable du traitement doit veiller à ce que les personnes travaillant sous son autorité n'aient accès et ne puissent utiliser que les données dont elles ont besoin pour exercer leurs fonctions. Il n'est pas question de permettre aux membres du personnel d'avoir accès à des données qui ne leur sont pas nécessaires[145].

Par exemple, les données à caractère personnel relatives à des employés peuvent être nécessaires aux personnes travaillant au sein d'un département ressources humaines. Par contre, seules certaines d'entre elles telles le nom, numéro de bureau, extension téléphonique par exemple sont utiles au réceptionniste.

85. Le responsable doit en outre mettre son personnel au courant des prescrits des dispositions légales en matière de protection des données[146]. Il doit expliquer les principes de protection qui doivent désormais être respectés. Cela peut, par exemple, être réalisé nous semble-t-il par des formations dispensées en interne ou par la mise à disposition d'un petit guide pratique, sur papier ou sur l'intranet, qui reprend les principes légaux à respecter.

86. En cas de sous-traitance d'un traitement effectué sur des données sensibles, le responsable du traitement devra prévoir une obligation de confidentialité à charge du sous-traitant[147].

B. Veiller à la sécurité des données

87. Le responsable du traitement est tenu de protéger les données contre une curiosité malsaine venant de l'intérieur ou de l'extérieur ou contre des manipulations non autorisées, qu'elles soient de nature accidentelle ou qu'elles soient malintentionnées. Il doit prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel[148].

---

145 Art. 16, § 2, 2° de la loi du 8 décembre 1992.
146 Art. 16, § 2, 3° de la loi du 8 décembre 1992.
147 *Cf.* section D, *infra*.
148 Art. 16, § 4 de la loi du 8 décembre 1992.

Ces mesures de sécurité que doit prendre le responsable du traitement sont donc de deux ordres : des mesures organisationnelles (limiter le nombre de personnes ayant accès aux données, fermer les locaux où sont localisés les ordinateurs et les fichiers, etc.) et des mesures techniques (protéger les bases de données contre les virus (programme anti-virus, *firewalls*), utiliser des droits d'accès - mots de passe et noms d'utilisateur -, cryptage, protection des locaux contre les incendies et dégâts des eaux, etc.).

La loi du 8 décembre 1992 précise que ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels. Plus les données en cause sont sensibles et les risques pour la personne concernée grands, plus importantes seront les précautions à prendre.

C. Prévoir certaines garanties en cas de sous-traitance

88. Le responsable de traitement peut confier l'exécution des opérations de traitement à un tiers sous-traitant. Le sous-traitant est donc « 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 »[149].

Le sous-traitant typique est le secrétariat social qui traite certaines données qui lui sont transmises par un employeur. On peut également citer l'exemple de la société informatique qui réalise un *back up* des données du responsable du traitement ou de la société de publipostage qui se charge de l'envoi de courrier sur la base d'une liste de destinataires établie par ses clients. T. Van Overstraeten cite également les tiers vers lesquels certains services tels que des *call centers*, des services informatiques ou *business process* sont externalisés (*outsourcing*)[150].

En revanche, les employés ne sont pas des sous-traitants de leur employeur[151].

89. Le responsable du traitement qui confie tout ou partie du traitement de données à caractère personnel à un sous-traitant doit s'assurer que celui-ci offre des garanties suffisantes au regard des mesures de sécurité technique et d'orga-

---

149 Art. 1, § 5 de la loi du 8 décembre 1992.

150 T. Van Overstraeten, « La protection des données à caractère personnel : quelques réflexions de praticien », *in Les 25 marchés émergents du droit*, (dir. L. Marlière), Bruxelles, Bruylant, 2006, pp. 357-358.

151 *Cf.* chapitre 2, *infra*.

nisation relatives aux traitements[152]. Il doit conclure avec ce dernier un contrat par écrit, sur support papier ou électronique, au sein duquel il est prévu que le sous-traitant veillera à appliquer ces mesures, qu'il n'agira que sur instruction du responsable du traitement et veillera à ce que son personnel respecte ce principe. Le contrat doit également fixer la responsabilité du sous-traitant vis-à-vis du responsable du traitement[153].

Section 4
Exigences propres à un traitement portant sur des données sensibles

A. Information spécifique en cas de traitement de données sensibles

90. Lorsque le responsable du traitement traite des données sensibles il doit fournir, outre les informations reprises *supra*[154], des informations supplémentaires, et ce qu'il ait obtenu les informations de la personne concernée ou d'un tiers.

Le responsable du traitement doit indiquer lors de l'information, si ce n'est déjà fait dans la déclaration à la Commission de la protection de la vie privée, la base légale (article de la loi du 8 décembre 1992) sur laquelle il se fonde pour traiter les données sensibles[155].

En outre, dans l'hypothèse où le traitement de ces données est exclusivement autorisé moyennant le consentement écrit de la personne concernée, le responsable du traitement doit lui indiquer les motifs pour lesquels ses informations sont traitées, ainsi que les catégories de personnes ayant accès à ses données[156].

B. Garanties supplémentaires

91. Des garanties supplémentaires sont à respecter également en cas de traitement de données sensibles :

– le responsable du traitement doit désigner les catégories de personnes ayant accès aux données et décrire de manière précise leur fonction par

---

152 Selon l'article 17, § 3 de la directive 95/46/CE, la loi de référence applicable pour déterminer quelles sont les obligations est la loi de l'État membre dans lequel le sous-traitant est établi. Voy. à cet égard, Groupe de l'Article 29, « Opinion 8/2010 on applicable law », WP179, 16 décembre 2010, p. 25, http://ec.europa.eu/justice/policies/privacy.

153 Art. 16, § 1 de la loi du 8 décembre 1992.

154 *Cf.* n° 79.

155 Art. 25, 4° de la loi du 8 décembre 1992.

156 Art. 26 de l'A.R. du 13 février 2001.

rapport au traitement des données[157]. Cela n'oblige pas le responsable du traitement à désigner les personnes par leur nom mais plutôt à établir des profils d'accès (le personnel de tel service, par exemple) ;

– de plus, les personnes traitant des données sensibles devront être tenues par une obligation de confidentialité qu'elle soit légale, statutaire ou contractuelle[158]. Celle-ci est également applicable au sous-traitant, lorsque le responsable confie la réalisation de certaines opérations de traitement à un tiers[159].

ÉTAPE 4
Se mettre en mesure de permettre un exercice effectif des droits des personnes concernées

92. Parallèlement aux conditions prescrites pour la mise en œuvre d'un traitement de données à caractère personnel, la loi du 8 décembre 1992 définit les droits dont bénéficient les personnes concernées.

Section 1
Droit à la curiosité

93. Nous avons évoqué ci-avant[160], l'obligation faite au responsable de traitement d'informer les personnes concernées à propos des traitements opérés sur les données les concernant.

94. Cette obligation de transparence est prolongée par le droit de toute personne à interpeller un responsable de traitement pour savoir s'il traite des données le concernant[161]. Le responsable ainsi interrogé doit confirmer s'il détient ou non des données et, dans l'affirmative, il a l'obligation de préciser dans quel but il détient ces données, de quelles catégories de données il s'agit et quels en sont les destinataires. Ainsi, un employé d'une filiale pourrait interpeller une autre société du groupe pour savoir si des données le concernant lui ont été communiquées.

95. Les personnes concernées disposent également d'un droit d'accès direct[162] aux données les concernant. Elles peuvent demander à recevoir, sous

---

157 Art. 25,1 de l'A.R. du 13 février 2001.

158 Art. 8, § 3 de la loi du 8 décembre 1992 et art. 25, 3° de l'A.R. du 13 février 2001.

159 Art. 25, 3° de l'A.R. du 13 février 2001 ; pour la notion de sous-traitant *cf.* n° 26 et 88.

160 *Cf.* n° 78 et s., *supra*.

161 Art. 10, a) de la loi du 8 décembre 1992.

162 Il existe également un droit d'accès indirect spécifique aux *données relatives à la santé* qui peut s'effectuer soit directement par la personne sur qui portent les données, soit par l'intermédiaire d'un profes-

une forme intelligible, une copie des données faisant l'objet d'un traitement ainsi que toute information disponible sur l'origine des données[163]. Le droit de connaître la provenance des données utilisées est particulièrement important car c'est bien souvent la question de la source des informations qui préoccupe les personnes concernées.

96. Dans le cas de décisions automatisées[164], la personne en cause doit pouvoir avoir aussi accès à la logique qui sous-tend le traitement automatisé en question[165].

97. Pour exercer son droit d'accès, la personne concernée doit, aux termes de la loi, adresser une demande au responsable du traitement en faisant la preuve de son identité (en joignant la photocopie de sa carte d'identité, par exemple). La demande doit être datée et signée et peut être envoyée par la poste ou par tout moyen de télécommunication (par fax, par courrier électronique avec apposition d'une signature électronique) ou être déposée sur place (dans ce cas la personne concernée doit se voir délivrer un accusé de réception).

Elle peut être adressée :

1° soit au responsable du traitement ou à son représentant, ses mandataires ou préposés ;

2° soit au sous-traitant du responsable du traitement qui la communique à l'une des personnes mentionnées sous 1°[166].

Il est évident que, dans le cadre d'une entreprise, il est possible et même sans doute préférable de mettre en place une procédure *ad hoc*, en indiquant par exemple la procédure interne à suivre et la personne au sein de l'entreprise à contacter.

98. Le responsable du traitement doit répondre sans délai et au plus tard dans les quarante-cinq jours de la réception de la demande et fournir une copie complète des données ainsi qu'un avertissement de la faculté d'exercer les recours prévus par la loi du 8 décembre 1992 et, éventuellement, de consulter le registre public de la Commission de la protection de la vie privée[167].

---

sionnel des soins de santé choisi par cette personne, si le responsable du traitement ou la personne elle-même demande l'intervention d'un intermédiaire. Ceci ne porte pas préjudice toutefois à l'application de la loi du 22 août 2002 relative aux droits du patient qui contient également des dispositions relatives à l'accès du patient à son dossier médical.

163 Art. 10, § 1, b) de la loi du 8 décembre 1992.

164 *Cf.* n° 58, *supra*.

165 Art. 10, § 1, c) de la loi du 8 décembre 1992.

166 Art. 32 de l'A.R. du 13 février 2001.

167 Art. 10, § 1, d) de la loi du 8 décembre 1992.

Il est toutefois prévu que le responsable de traitement ne doit donner suite à une nouvelle demande d'accès qu'à l'expiration d'un délai raisonnable, à compter de la date d'une demande antérieure d'une même personne à laquelle il a été répondu ou de la date à laquelle les données lui ont été communiquées d'office[168].

Section 2
Le droit de rectification

99. Chacun peut, sans frais, faire rectifier les données inexactes qui se rapportent à lui et faire effacer ou interdire d'utilisation les données incomplètes, non pertinentes ou interdites[169].

Les modalités d'exercice du droit de rectification sont identiques à celles prévues pour l'accès aux données[170]. Le responsable du traitement doit répondre dans le mois à celui qui a demandé les corrections. Il doit indiquer les rectifications ou effacements qu'il a effectués. S'il ne le fait pas, la personne concernée peut dénoncer ce comportement à la Commission de la protection de la vie privée, voire initier une procédure en justice[171].

Si des données inexactes, incomplètes, non pertinentes ou interdites ont été transmises à des tiers, le responsable doit, dans le mois, signaler les corrections ou effacements à effectuer aux personnes à qui ces données ont été communiquées, à moins que cela ne s'avère impossible ou extrêmement difficile[172].

Section 3
Le droit d'opposition

100. La personne concernée a le droit de s'opposer à ce que les données la concernant fassent l'objet d'un traitement, mais elle doit invoquer des raisons sérieuses et légitimes. Le responsable de traitement ne peut plus traiter les données de la personne concernée si l'opposition est justifiée.

Le droit d'opposition n'est cependant pas admis pour les traitements nécessaires à la conclusion ou à l'exécution d'un contrat ou lorsque le traitement est imposé par une obligation légale ou réglementaire[173].

---

168 Art. 10, § 3 de la loi du 8 décembre 1992.
169 Art. 12, §§ 1 et 2 de la loi du 8 décembre 1992.
170 Art. 33 de l'A.R. du 13 février 2001.
171 *Cf.* art. 13 à 15*bis* de la loi du 8 décembre 1992.
172 Art. 12, § 3 de la loi du 8 décembre 1992.
173 Art. 12, § 1 de la loi du 8 décembre 1992.

Les modalités d'exercice du droit d'opposition sont identiques à celles prévues pour l'accès aux données[174]. Le responsable du traitement doit indiquer dans le mois la suite réservée à l'exercice du droit d'opposition.

Conclusion

101. Permettre un exercice effectif de ces droits implique que le responsable de traitement en tienne compte lors de l'organisation des traitements qu'il entend mettre en œuvre.

Ainsi, si les données traitées sont éparpillées au sein de différentes bases de données, il sera plus difficile de donner suite à une demande d'accès ou de s'assurer que les demandes de rectifications seront correctement exécutées pour toutes les données qui se trouvent traitées ci et là dans l'entreprise.

Chapitre 2
Le travailleur acteur de traitements

102. Le travailleur peut être amené à opérer des traitements de données à caractère personnel. Comme il a été précisé ci-avant, le préposé qui participe aux traitements de données dans le cadre du travail qu'il accomplit pour son employeur n'a pas la qualité de responsable de traitement, ni même celle de sous-traitant[175].

Il convient donc de s'assurer que les traitements entrent dans le cadre de l'exécution du contrat de travail.

> Ainsi, si un travailleur effectue des traitements à caractère personnel pour l'exécution d'un projet qui lui est confié par son employeur, c'est ce dernier qui est le responsable du traitement. Ceci prévaut quand bien même c'est l'employé qui, en définitive, décide des finalités et des moyens à mettre en œuvre dans l'exécution du travail. En revanche, si l'employé procède à des traitements de données à caractère personnel dans le cadre d'activités effectuées hors contrat de travail, pour son propre compte (rédaction d'un ouvrage à titre personnel par exemple), il est le responsable des traitements réalisés dans ce contexte.

174 Art. 33 de l'A.R. du 13 février 2001.

175 Art. 1, § 2, 5° de la loi du 8 décembre 1992. Voy. en ce sens : Th. Léonard, « La Protection des données à caractère personnel et l'entreprise », *Guide Juridique de l'entreprise*, Titre XI, livre 112.1, p. 18.

Il incombe à l'employeur responsable de traitement de s'assurer de la légalité des opérations de traitement mises en œuvre par ses préposés, qu'il s'agisse de préposés ou de fonctionnaires.

> Ainsi, par exemple, si des délégués commerciaux prennent l'initiative de constituer des fichiers clients dans lesquels ils intègrent des informations relatives aux personnes de contact, en ce compris des données relatives à la vie privée de ces personnes, c'est l'employeur qui doit être considéré comme responsable de ces traitements. Il appartient donc à l'employeur de s'assurer une certaine maîtrise sur les informations collectées par ses préposés. Sont donc à proscrire des collectes de données faites à l'initiative des travailleurs et qui seraient étrangères aux finalités de traitement, ainsi que des données relatives à la vie privée des personnes de contact qui, si elles permettent peut-être d'avoir des contacts plus personnalisés avec la clientèle, ne se justifient pas forcément. Il est d'ailleurs généralement fait l'impasse sur le respect de l'obligation d'information. On imagine mal une entreprise commerciale informer les personnes de contact chez ses clients qu'elle conserve dans des fichiers des données relatives à leur situation familiale, etc.

La loi du 8 décembre 1992 se montre particulièrement stricte sur la marge de manœuvre du travailleur. L'article 16, § 3 de cette loi prévoit, en effet, que «Toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance». Autrement dit, la loi exige, nous semble-t-il, que toutes les opérations de traitement effectuées par des préposés n'interviennent que suivant les instructions spécifiques de l'employeur.

103. Par ailleurs, l'employeur en sa qualité de responsable de traitement, a également l'obligation d'informer les personnes agissant sous son autorité des dispositions de la présente loi et de ses arrêtés d'exécution, ainsi que de toute prescription pertinente, relative à la protection de la vie privée a l'égard des traitements des données à caractère personnel[176].

104. Sur le plan de l'organisation d'un traitement de données à caractère personnel, certaines règles intéressent également les préposés. Ainsi le responsable du traitement doit-il veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service[177]. En outre, dès lors que ces préposés

176 Art. 16, § 2, 3° de la loi du 8 décembre 1992.
177 Art. 16, § 2, 3° de la loi du 8 décembre 1992.

sont amenés à traiter des données sensibles, leur employeur, toujours en sa qualité de responsable de traitement, doit veiller à ce qu'elles soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données[178]. Il aura d'ailleurs dû déterminer les catégories de personnes qui auront accès à ces données sensibles. Le responsable de traitement est en effet tenu d'établir une liste des catégories des personnes qui bénéficient de cet accès et de décrire leur fonction par rapport au traitement des données en cause[179]. Cette liste doit être fournie sur demande à la Commission de la protection de la vie privée.

105. À la lecture de ces différentes dispositions, on perçoit toute l'ambigüité que peut revêtir la législation quant aux obligations respectives des parties. L'employeur, en tant que responsable du traitement, doit s'assurer de la légalité de celui-ci et notamment dûment informer ses préposés sur les tenants et aboutissants de la loi. Dans le même temps, le préposé n'est censé agir que sur la base des instructions du responsable du traitement mais doit lui-même respecter les dispositions de la loi du 8 décembre 1992. Il est en effet à noter que, nonobstant le fait que le préposé n'a pas la qualité de responsable de traitement, cela ne l'exempte pas de toute responsabilité en cas de non-respect de la loi. En marge du régime de responsabilité du travailleur, les articles 38 et 39 de loi du 8 décembre 1992 érigent en infractions pénales la violation de la plupart des dispositions de la loi et vise également, dans les personnes susceptibles d'être sanctionnées, les préposés.

Conclusion

106. Dès lors qu'un employeur traite, en tant que responsable de traitement, des données (informations écrites, photographies, images vidéo, empreintes digitales,…) relatives à ses travailleurs, qu'il s'agisse d'un enregistrement, d'une communication ou de la simple conservation de données à caractère personnel, il est tenu de se conformer aux conditions qui permettent de garantir la transparence et la légitimité des traitements.

107. Pour assurer la transparence du traitement, l'employeur devra fournir certaines informations aux travailleurs - notamment en ce qui concerne le but poursuivi par le traitement - et faire une déclaration du traitement auprès la Commission de la protection de la vie privée sauf s'il peut se prévaloir

178 Art. 25, 3° de l'A.R. du 13 février 2001.

179 Art. 25, 1° et 2° de l'A.R. du 13 février 2001.

des exceptions prévues par la loi. Ensuite, concernant la mise en œuvre du traitement, l'employeur doit respecter certains principes : le traitement devra toujours être loyal et licite, tandis que les finalités de traitement doivent être déterminées, spécifiques et légitimes. La loi du 8 décembre 1992 dresse une liste des cas dans lesquels les finalités de traitements sont *a priori* légitimes (par exemple lorsqu'elles sont nécessaires à l'exécution d'un contrat). Les données collectées devront être adéquates, pertinentes et non excessives par rapport aux finalités de traitement poursuivies. L'employeur ne pourra traiter des données à caractère personnel (au lieu de traiter des données anonymes par exemple) que lorsque cela est nécessaire au regard du but poursuivi par le traitement. Ce principe implique également que les données doivent être effacées ou rendues anonymes dès qu'elles ne sont plus nécessaires. Enfin, les données ne pourront en principe être traitées que pour les finalités annoncées au travailleur ou pour des finalités compatibles avec celles-ci.

Si l'employeur se plie à ces conditions, il peut traiter des données à caractère personnel à l'exception des données dites « sensibles ». Ces données ne peuvent pas être traitées sauf dans les cas spécifiquement admis par la loi du 8 décembre 1992 et moyennant le respect d'obligations et de garanties complémentaires. Certaines restrictions demeurent pour assurer le maintien d'un niveau de protection adéquat (régime des flux transfrontières) ou un équilibre entre les intérêts des parties (régime des décisions automatisées).

Par ailleurs, la loi du 8 décembre 1992 reconnaît aux personnes dont les données font l'objet d'un traitement un droit d'accès aux données, un droit de rectification et un droit d'opposition au traitement pour des motifs sérieux et légitimes tenant à sa situation particulière. L'employeur doit donc assurer la possibilité d'un exercice effectif de ces droits.

Enfin, tout responsable de traitement doit prendre des mesures techniques et organisationnelles pour assurer la sécurité et l'intégrité des données ainsi que le respect de la loi du 8 décembre 1992 par son personnel.