- Renforcement du devoir d'informer quant à la collecte de *données sensibles* et de *profils de la personnalité.* Les articles 4, 7a et b touchent particulièrement les traitements informatiques tels que le *Data Mining.*

- Abandon de l'obligation de déclarer au *PFPD* pour les personnes privées traitant régulièrement des *données sensibles* ou des *profils de la personnalité* ou qui communiquent régulièrement des *données personnelles* à des tiers.

- Obligation pour le *Maître de fichier* de suspendre immédiatement le traitement lorsque la personne concernée s'y oppose.

- Adaptation des dispositions pénales quant à l'obligation de renseigner, de l'omission de fournir des données, de leur fourniture inexacte ou incomplète par le *Maître du fichier*.

5. Résumé et Conclusion

Nous étudiâmes la mise sur pied et l'exploitation d'un système appréhendant le *Risque Humain* au moyen d'un *Tableau de Bord* utilisable dans le *Risk Management*. Ce *Tableau de bord* fournit des *indicateurs préventifs et détectifs* quant aux *risques opérationnels* pouvant induire un *dysfonctionnement humain*, qu'il soit accidentel ou volontaire. Ce dernier critère peut être subdivisé en deux sous-catégories : avec ou sans intention délictueuse. La *détection* et la *prévention* d'intentions délictueuses sont plus difficilement maîtrisables d'une manière *directe.* Une telle approche suppose l'accès permanent à des *données personnelles, des données sensibles et des profils de la personnalité,* qu'ils proviennent de sources internes ou externes à l'entreprise. Il est plus aisé d'agir en amont, en prévenant les *flous* évoqués au *chapitre 2. Méthodologie et Mise en œuvre du Management Matriciel*. L'élimination de ces *flous*, en travaillant sur les axes *Compréhension, Compétence, Satisfaction* et *Organisation,* constitue un moyen préventif efficace. Ceci empêchera d'une manière perceptible les *dysfonctionnements* non délictueux et peut prévenir la germination et le déploiement d'énergies criminelles diffuses. A défaut, l'élimination des *flous* permettra de contenir ces énergies à un stade précoce, en agissant sur les éléments fondamentaux que sont *l'auteur, l'outil/le moyen et l'opportunité (point 1.3.4. Les causes du Risque Humain*).

Dans ce but, nous évoquâmes une méthode appelée *Management Matriciel*. Par un processus d'*autoévaluation* continue, elle consiste à déterminer les *Besoins* et à les traiter, si nécessaire, à l'aide d'une *Analyse des risques*. Les résultats sont consignés dans une matrice formalisant les *Exigences,* ces derniers aboutissant à une deuxième matrice appelée *Plan d'action.* Celle-ci est structurée selon le cycle *PDCA* (Plan, Do, Check, Act), en application du principe de la *Roue de Deming.* Afin d'éliminer les *non-dits* entre les participants de la chaîne organisationnelle, on appliquera la *Méthode du Miroir,* consistant à déterminer les *perceptions* et *attentes* réciproques. A l'aide de *référentiels* mis au point par les participants au système, il sera possible de connaître en tout temps le *taux d'atteinte de l'exigence/de l'action* et les *valeurs relatives à l'exploitation du système.*

Cette méthode a l'avantage d'une mise en oeuvre à tout moment, sans que l'on dispose nécessairement d'une vue de l'ensemble des *Besoins* nécessaires à l'entreprise. Si au départ la méthode demeure imparfaite, le processus, quant à lui, est parfait, grâce au cycle automatique

consistant à corriger et adapter les *Exigences* d'une manière continue. Le système s'*autoperfectionne* donc au fur et à mesure.

Techniquement ce système est exploité dans un environnement de *Data Warehousing.* Il peut être complété, dans des limites légales bien définies, par le traitement de données issues de différentes bases de données opérationnelles En fonction de la granularité souhaitée, on pourrait *remonter* jusqu'à l'individu. De plus et au moyen de logiciels spécifiques de *Data Mining* il est possible d'extraire des *données implicites* et de les transformer en *informations explicites*, donc potentiellement *individualisables.*

La consolidation finale de ces informations dans un *domaine* du *Risque Humain* (exemple : *Satisfaction*) et moyennant une segmentation prédéfinie (exemple : Département X, *service XY, groupe A, équipe 12, etc*), apparaîtra au *Tableau de bord,* sous forme d'*indicateurs*.

Si envisagé par le *Risk Management*, le système peut être complété par des modèles préétablis et actualisés régulièrement à l'aide de bases de données internes et/ou externes, provenant des domaines Ressources Humaines et Audit notamment. Ces modèles alimenteront et affineront les *indicateurs* du *Tableau de Bord de la Veille Humaine*. Comme mentionné au premier paragraphe de ce chapitre, ils sont censés couvrir, cas échéant, les intentions délictueuses. Une telle approche implique l'exploitation de données juridiquement délicates.

Les interprétations au niveau de la doctrine divergent parfois des prises de position du *PFPD.* Le Droit ayant notoirement un temps de retard sur les évolutions technologiques, organisationnelles et sociologiques, les implications du *Data Warehousing* en général et de notre approche de la *Veille Humaine* en particulier, manquent de références juridiques. Le recours à des textes de jurisprudence ou de doctrine demeure de ce fait quelque peu hasardeux. A notre connaissance, nous ne disposons pas de suffisamment de cas spécifiques pouvant s'appliquer à notre étude. Il s'agirait donc, pour l'instant, de démontrer *bonne foi, proportionnalité* et *intérêt prépondérants.*

Il n'en demeure pas moins que selon *OLT 3, section 5, art 26,* « (…) il est interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leurs postes de travail » sauf « (…) s'ils sont nécessaires pour d'autres raisons » *(sécurité des travailleurs ou de l'entreprise, performance)*. Il n'est pas exclu que la *Veille Humaine* conçue sous cette forme soit apparentée à un *système de surveillance ou de contrôle du comportement,* notamment s'il est fait recours à des *indicateurs* incluant la mesure de comportements *erronés* ou *inhabituels.* Les chances d'échapper à une telle interprétation nous paraissent meilleures si l'*individualisation* des données est rendue techniquement impossible, notamment pour celles dont la *Loi sur la protection des données* (*LPD)* révisée risque d'exiger à l'avenir le *consentement explicite* de la personne concernée. Une interprétation plus large des *autres raisons* permettrait de justifier cette démarche en invoquant l'argument de *sécurité* et de *performance* sous l'angle préventif, en visant la protection de l'entreprise et de ses employés.

Le concept de la *Veille Humaine* doit être piloté sous forme d'un projet avec un ou plusieurs coordinateurs appelés à assurer la compréhension et l'exécution homogène de chaque processus. En fonction de la taille de l'entreprise, cette tâche incombera à un organisateur interne, assisté d'un spécialiste externe.

Pour garantir le bon fonctionnement du système, la *confiance* du personnel et l'*information* en sont les clés de voûte. Ainsi, les *aspects éthiques et juridiques* doivent s'inscrire dans un *contexte culturel* interne et externe. Une *transparence* absolue à l'égard du personnel est indispensable, de même qu'une *politique de communication* circonstanciée. Une instance de *compliance* veillera au respect des *normes éthiques et juridiques.*

Pour notre part, nous sommes d'avis que la *Veille Humaine* doit être conçue de telle manière qu'il sera impossible d'exploiter les *indicateurs du Tableau de bord* jusqu'au niveau de la personne. Cette politique facilitera grandement l'*adhésion* et l'*implication* des personnes concernées à sa mise sur pied et à son exploitation. Il faut en effet garder à l'esprit que le cœur du système repose sur l'*autoévaluation* à plusieurs niveaux. Ainsi, on évitera les écueils juridiques liés à la *LPD* et on rendra la politique de communication plus aisée.

D'entente avec l'instance de *compliance* susmentionnée, le *Risk Manager* veillera à l'établissement, à la communication et au respect d'une procédure réglant les *accès restrictifs* aux différentes bases de données du système.

La *Veille Humaine* consiste à observer et à analyser la *Ressource Humaine* pour elle-même et par rapport à son environnement. Alors que les *Veilles Scientifique, Technique, Technologique et Economique* sont surtout tournées vers l'extérieur, le sujet qui nous occupe correspond principalement à une *Veille Interne*. L'exploitation d'un système d'informations actualisées permet d'optimiser sa mise en valeur. Par ce biais, on conserve, respectivement on accroît l'avantage concurrentiel de l'entreprise. Parallèlement, ce système distille des informations permettant l'atteinte d'un double effet : l'anticipation débouche sur une *plus-value* du capital humain et prévient les dommages causés par un comportement inadéquat du personnel.