L'IMMATERIEL ET LA PROTECTION DE LA PERSONNE

Programme d'économie-droit – Sections de technicien supérieur - Tertiaire

Thème 4 : l'immatériel dans les relations économiques

Il est nécessaire d'avoir étudié le thème relatif aux relations contractuelles avant d'aborder l'étude de l'immatériel dans les activités économiques.
Les activités économiques présentent une tendance nette au développement de l'immatériel. Par ce dernier terme il faut entendre ce qui est incorporel c'est-à-dire « ce qui ne peut pas être touché, ce qui ne tombe pas sous les sens ». Ce thème repose sur l'idée que l'immatériel est aujourd'hui nécessaire au développement des activités économiques et contribue à la création de valeur. Les courants d'affaires passent, de plus en plus souvent, par des flux d'informations dématérialisés échangés par des partenaires potentiels.
Ces flux se rencontrent dans la phase de négociation comme dans la phase de formation des relations d'affaires.
Il convient de limiter l'étude aux principes généraux qui régissent l'immatériel dans les relations économiques et, plus particulièrement, d'éviter tout développement à caractère technique dans le traitement de ce thème. Enfin, le choix est fait de ne pas aborder les éléments immatériels tels que le fonds de commerce et les brevets.

Compétences :

- **Apprécier la légalité d'une situation au regard de la protection de la personne dans la sphère privée et professionnelle**
- **Caractériser les éléments principaux de cette protection et son évolution**
- **Rédiger et qualifier quelques clauses d'un document relatif à l'usage des TIC**

423. L'immatériel et la protection de la personne

- Données à caractère personnel : notion, traitement, règles de protection des droits de la personne, obligations des responsables du traitement, organes de contrôle (423-1)

INDICATIONS COMPLEMENTAIRES
(423-1) *Il s'agit, après avoir fait un rappel de ces notions, de montrer que les TIC démultiplient les risques d'atteintes aux droits et libertés des individus. En se fondant sur la protection des données à caractère personnel on peut montrer pourquoi et comment le droit met en place des autorités de régulation. Il faudra souligner que cette protection se fait nécessairement dans le cadre communautaire et national.*

- Respect des données à caractère personnel collectées lors de conclusion et de l'exécution du contrat de travail. (423-2)

INDICATIONS COMPLEMENTAIRES
(423-2) *L'employeur peut dans le cadre de ses pouvoirs apporter certaines restrictions à l'usage des technologies de l'information et de la communication par ses salariés. Il faut montrer comment, les pouvoirs de contrôle et de surveillance peuvent être mis en œuvre de manière adaptée aux nouvelles technologies mais toujours contraints par la garantie des libertés fondamentales.*

L'IMMATERIEL ET LA PROTECTION DE LA PERSONNE

Encore ignorée il y a une dizaine d'années, l'économie numérique est désormais en marche. La société de l'information est appelée de tous vœux à supplanter les schémas traditionnels de commerce, de communications et d'échanges.
Lors de la révolution industrielle, c'était le bien qui était le fondement même du système, avec la révolution numérique, c'est l'information. Un progrès n'est pourtant jamais sans conséquence néfaste ! L'industrialisation a apporté la pollution de l'environnement, l'informatique fait craindre une destruction de la vie privée.
C'est le 21 mars 1974 qu'est mis le feu aux poudres ! Le projet SAFARI de l'INSEE était alors dénoncé dans le journal *Le Monde* sous le titre : « *SAFARI ou la chasse aux Français* ».
Cette affaire a eu un effet retentissant, non seulement en raison de la maladresse inconsciente dans le choix du sigle, mais aussi parce que le numéro de l'INSEE est couvert d'un voile de suspicion depuis sa création pendant la deuxième guerre mondiale, du fait de son utilisation nauséeuse par l'administration de l'époque.

Qu'en est-il 30 ans plus tard ?

D'une part, on a assisté à la création en France de la CNIL en 1978 et, en Europe, l'implication progressive du conseil européen et la création du G29 (composé des CNIL européennes) ont démontré la volonté de l'Europe de prendre en considération le problème.

D'autre part, l'actualité florissante nous effraye ! Novembre 2007 : des cédéroms contenant les données bancaires de 25 millions de contribuables sont égarés par les services fiscaux britanniques...
Août 2008 : un ordinateur contenant les données bancaires d'un million de clients britanniques est vendu pour 44 euros sur le site d'enchères eBay...
Dans le même temps, le ministère des Finances britannique égare un fichier comportant les noms des 84 000 prisonniers, dont ceux de 10 000 personnes «à surveiller en priorité pour leur comportement délictueux prolifique»...

Ces failles de sécurité, graves, ont démontré que la sécurité et, de façon plus générale, la protection des données n'étaient malheureusement toujours pas prises au sérieux par les entreprises et les administrations. En parallèle, les acronymes se multipliant au fil du temps (NIR, STIC, EDVIGE, SIS, GEVI, FNAEG, ARIANE, FAR, FIJAIS,…), notre société semble alors de plus en plus verser dans le panoptisme.

Ce constat est le résultat de la réunion de trois évolutions majeures qui sont apparues dans la seconde moitié du XX^{ème} siècle. D'une part, il y a eu l'affirmation du respect dû à la vie privée (*Convention européenne des droits de l'Homme - 4 novembre 1950*), puis l'apparition de l'informatique et, enfin, la tertiarisation de l'économie et l'accroissement du rôle de l'Etat qui ont provoqué la multiplication des fichiers informatiques.

Au niveau économique, l'immatériel est devenue une valeur essentielle et les nouvelles formes de travail « imposées » par l'informatique engagent également les entreprises dans ce processus de traitement de données et donc de protection parfois difficile.

Nous étudierons dans une première partie l'évolution du risque engendré par les nouvelles technologies sur les données à caractère personnel puis, nous ferons un point sur l'état du droit au niveau national et européen. Enfin, dans une troisième partie, nous observerons plus précisément le cas des entreprises au sein desquelles les données à caractère personnel jouent un rôle primordial.

I. Les TIC : un risque démultiplié pour les données à caractère personnel

■ **Rappel des notions** (TIC, Données à caractère personnel)

- Les **technologies de l'information et de la communication** (**TIC** ou *NTIC* pour *« Nouvelles Technologies de l'Information et de la Communication »* regroupent les techniques utilisées dans le traitement et la transmission des informations, principalement de l'informatique, de l'internet et des télécommunications.
Les usages des TIC ne cessent de s'étendre, surtout dans les pays riches, au risque localement d'accentuer la fracture numérique et sociale ainsi que le fossé entre les générations. De l'Agriculture de précision et de la gestion de la forêt (traçabilité des bois pour lutter contre le trafic), au monitoring global de l'environnement planétaire ou de la biodiversité, à la démocratie participative (*TIC au service du développement durable*) en passant par le commerce, la télémédecine, l'information, la gestion de multiples bases de données, la bourse, la robotique et les usages militaires, sans oublier l'aide aux handicapés, les TIC tendent à prendre une place croissante dans la vie humaine et le fonctionnement des sociétés. Certains craignent ainssi une perte de liberté individuelle. Les prospectivistes s'accordent à penser que les TIC devraient prendre une place croissante et pourraient être à l'origine d'un nouveau paradigme civilisationnel.

- Les **données personnelles** sont les informations qui permettent d'identifier directement ou indirectement une personne physique. Les données personnelles (ou nominatives) correspondent aux noms, prénoms, adresses (physique et électronique), numéro de téléphone, lieu et date de naissance, numéro de sécurité sociale, etc. Certaines de ces données, dont en particulier le numéro de sécurité sociale ou le NIR, ainsi que les données biométriques (empreinte digitale, échantillon ADN, etc.), sont particulièrement sensibles, car elles fonctionnent en tant qu'« identifiants universels », qui permet de raccorder différents fichiers entre eux et ainsi d'opérer leur interconnexion.
Toutes les données sont-elles devenues personnelles ? C'est la question posée par David Brin (***The Transparent Society*** - 1998). En effet, la dichotomie plaçant d'un côté des données personnelles et de l'autre des données qui ne le sont pas est erronée selon lui. Un très grand nombre de données apparemment anonymes peuvent en fait devenir personnelles après traitement.
Se pose encore à l'heure actuelle la question de savoir si les traces numériques (cookies, etc.) doivent être considérées comme étant des données personnelles. Le fait est que certains permettent d'obtenir des renseignements sur les habitudes de navigation des internautes, opérant ainsi une collecte d'informations personnelles à l'insu du visiteur d'un site et permettant l'élaboration ultérieur de profils, utilisés notamment à fins publicitaires ou/et commerciales (ciblage comportemental), mais pouvant aussi être utilisés dans le cadre d'enquêtes judiciaires. L'adresse IP, elle, n'est pas considérée comme une donnée personnelle, depuis un arrêt de la Cour de cassation (13 janvier 2009).

■ L'évolution des TIC et la multiplication des fichiers informatiques

La question que se pose Alex Türk (*Président de la CNIL*) dans l'avant-propos du 29ème rapport de la CNIL (2008) et la réponse qu'il y donne sont révélateurs de cette évolution : « […] *quelle marque laissera donc cette année 2008 dans la mémoire commune de l'ensemble des membres de l'équipe CNIL, commissaires et personnel ? S'il me faut choisir, je crois que ce qui restera imprimé, c'est ce constat selon lequel plus aucun secteur d'activité, plus aucune parcelle de notre vie individuelle et collective, n'échappe désormais au développement et à la pression des technologies nouvelles de l'information.* […] »

La loi (de 1978) doit, tel un organisme vivant, s'adapter aux évolutions de son environnement (les nouvelles technologies évoluent à une vitesse extraordinaire). Il y a une sorte de « darwinisme » de la loi selon Jean Frayssinet (*Professeur à l'Université Paul Cézanne - Aix-Marseille III - Directeur de l'IREDIC*).

C'est cette évolution fulgurante qui menace les donnés à caractère personnel en les mettant face à des risques de plus en plus nombreux car les réseaux informatiques sont interconnectés les uns aux autres et démultiplient donc l'information.

De plus, les technologies semblent toujours avoir une longueur d'avance sur les lois. Ainsi, alors que les réseaux sociaux pullulent et que les dégâts semblent déjà bien établis, quelques députés demandent la mise en place d'un « droit à l'oubli ». Sur ce point, Jean Frayssinet écrit que l'individu ne doit pas être gêné « *toute sa vie durant par des informations fichées et utilisées à son insu*». Il continue en soulignant qu'il s'agit d'un droit « *à l'habeas data ou d'un droit à l'oubli* ».

Le risque est donc bien présent et semble s'étendre rapidement…

II. Face au risque, la riposte du Droit national et européen

■ Au niveau du droit national

- La loi n° 78-17 du 6 janvier 1978

La Commission nationale de l'informatique et des libertés (CNIL) est une autorité administrative indépendante française chargée de veiller à la protection des données à caractère personnel et de la vie privée. Elle a été créée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Rappelons simplement les missions de la CNIL qui s'orientent autour de trois axes :

- **l'information** : la CNIL informe les autorités publiques et les professionnels mettant en œuvre des traitements de données nominatives sur leurs devoirs, et les citoyens sur leurs droits. Elle permet aussi aux citoyens d'exercer leur droit d'accès dit indirect à certains fichiers (ex. : fichier des renseignements généraux). Les moyens utilisés pour cette information sont notamment son site internet (pour l'information générale sur la loi et ses modalités d'application), le rapport annuel, la publicité faite sur des délibérations clés (via la presse), l'organisation de réunions thématiques régionales à destination des professionnels.
- **le contrôle** : le contrôle du respect de la loi s'effectue *a priori* (par l'instruction des dossiers de déclaration) et *a posteriori* (par des visites dans les entreprises et organismes, suite à une plainte ou non).
- **la répression** : les pouvoirs de sanction conférés par le législateur sont l'avertissement, la mise en demeure et la sanction financière. La CNIL peut aussi saisir le parquet dans les cas les plus graves.

La loi du 6 août 2004 a modifié la loi de 1978 en transposant librement en droit français la directive européenne du 24 octobre 1995 sur la protection des données à caractère personnel. La loi de 2004 allège de façon substantielle les obligations déclaratives des détenteurs de fichiers, accroît les pouvoirs de la CNIL en ce qui concerne les investigations sur place et les sanctions, et renforce les droits des personnes.

La loi française relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 a été incorporée, en 1995, par le Conseil constitutionnel, dans le socle des libertés publiques dotées d'une garantie constitutionnelle.

L'activité grandissante de la CNIL qui ne cesse d'apparaître dans les titres de la presse quotidienne (*cf : les recommandations actuelles en ce qui concerne les plans de continuité de l'activité – PCA – face à la grippe H1N1*) prouve tout l'intérêt de sa création en 1978.
Néanmoins, les pouvoirs de la CNIL ont été diminués en ce qui concerne les fichiers visant à la sécurité nationale ou à la défense du territoire, ceci à la demande du gouvernement Raffarin, et avec l'accord du président de la Cnil, Alex Türk. De plus, la loi du 23 janvier 2006 relative au traitement du terrorisme a également diminué ses pouvoirs, puisqu'elle « permet désormais de limiter, sous certaines conditions, l'information communiquée à la CNIL lorsqu'elle rend un avis sur les fichiers intéressant la sûreté de l'Etat, la défense ou la sécurité publique. »

- **La loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004**

Cette loi fait suite à la directive européenne du 8 juin 2000 sur le commerce électronique. La transposition aurait dû être effective le 17 janv. 2002 mais ne l'aura été que le 21 juin 2004.
Cette loi comporte 58 articles qui instituent un nouveau cadre juridique à Internet. Tous les acteurs d'Internet sont abordés : éditeurs de site, internautes, prestataires techniques, consommateurs, vendeurs…
Les quatre axes importants de la LEN sont : l'institution d'une liberté de communication en ligne, l'encadrement du commerce électronique, la publicité par voie électronique et la lutte contre la cybercriminalité.

■ Au niveau du droit européen

Dès 1973, la Suède avait ouvert la voie en se dotant d'une loi protégeant les personnes contre un usage abusif de l'informatique. Le Land de Hesse, en Allemagne, avait suivi, précédant de peu la France. Ces lois, et - pourquoi ne pas le reconnaître, la loi française - ont inspiré la première convention internationale sur le sujet : la Convention du 28 janv. 1981 du Conseil de l'Europe, dite "**convention 108**". Cette convention, qui est "la sœur cadette" de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, est aujourd'hui ratifiée par vingt Etats. Très au-delà de l'Europe, des pays aussi différents que le Canada, Singapour, l'Australie, la Nouvelle-Zélande, Hong Kong, le Japon, Israël, se sont également dotés de lois "informatique et libertés", même si leur champ d'application est le plus souvent limité aux seuls fichiers publics. Enfin, il est frappant de constater l'impatience qu'ont manifestée nos voisins du Centre et de l'Est européen à se doter de telles lois en signe d'affranchissement du joug des années noires : République Tchèque (1992), Lituanie (1996), Pologne et Hongrie (1997), Lettonie (1998). Ni la Russie, ni la Roumanie ne manquent à l'appel. On doit se réjouir de cette liberté qui essaime.

La protection des données : pourquoi ?

L'utilisation croissante du traitement automatisé des données à caractère personnel au cours des dernières décennies n'a fait qu'accroître le risque d'utilisation illicite ou illégale des données à caractère personnel et faciliter leur transfert par-delà les frontières entre pays avec des niveaux de protection très différents pour ces données.
Or, la Convention européenne des Droits de l'Homme garantit un certain nombre de droits civils et politiques, parmi lesquels le droit à la vie privée (article 8) et le droit à l'information (article 10), deux droits potentiellement conflictuels.

Face à la nécessité de concilier ces deux droits fondamentaux et de garantir le même niveau de protection pour ces droits au-delà des frontières nationales, le Conseil de l'Europe a élaboré une "Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel" qui a été ouverte à la signature le 28 janv. 1981. A l'heure actuelle, elle reste dans ce domaine le seul instrument juridique contraignant sur le plan international, à vocation universelle, ouverte donc à l'adhésion de tout pays y compris non-membre du Conseil de l'Europe.

La Convention pour la protection des données de 1981

Cette Convention définit un certain nombre de principes pour que les données soient collectées et utilisées de façon loyale et licite. Ainsi, elles ne peuvent être collectées que dans un but précis et ne peuvent être utilisées de manière incompatible avec ce but ; elles doivent être exactes, proportionnées à cet objectif et conservées uniquement pendant le délai nécessaire à sa réalisation. Le texte établit, en outre, le droit d'accès et de rectification de la personne concernée et exige une protection spéciale pour les données sensibles.
Pour devenir partie à la Convention, les Etats doivent garantir que leur législation nationale énonce ces principes de base à l'égard des données à caractère personnel relatives à tous les individus résidant sur leur territoire. Dès lors qu'un niveau de protection (minimum) commun est ainsi créé, la libre circulation des données à caractère personnel entre les Etats parties à la Convention est autorisée.

De la théorie à la pratique

Afin d'adapter les principes généraux énoncés dans la Convention aux exigences spécifiques des différents secteurs d'activité de la société, plusieurs recommandations ont été adoptées par le Conseil de l'Europe dans différents domaines : les banques de données médicales automatisées (1981), la recherche scientifique et de statistiques (1983), le marketing direct (1985), la sécurité sociale (1986), les fichiers de police (1987), les données utilisées à des fins d'emploi (1989), les paiements et autres opérations connexes (1990), la communication à des tierces personnes de données détenues par des organismes publics (1991), la protection des données à caractère personnel dans le domaine des services de télécommunications, notamment des services téléphoniques (1995), la protection des données médicales et génétiques (1997), la protection des données personnelles collectées et traitées à des fins statistiques (1997), sur la protection de la vie privée sur Internet (1999).

De même, les directives concernant la protection des données personnelles se multiplient :

- Directive du 12 juillet 2002 concernant le traitement des données à caractère personnel *et la protection de la vie privée* transposée en France dans la loi LEN de 2004.
- Directive du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques.

Rappelons enfin l'existence du **Groupe de travail « Article 29 » ou « G29 »** qui est un organe consultatif européen indépendant sur la protection des données et de la vie privée.
Ses missions sont les suivantes :

- Conseiller la Commission européenne, et lui donner un avis autorisé, sur toute mesure communautaire ayant une incidence sur les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel et de la protection de la vie privée.
- Promouvoir une application uniforme des directives européennes au moyen de la coopération entre les autorités de contrôle de la protection des données.
- Émettre des recommandations destinées au grand public.

III. Focus sur la gestion de ce risque par les entreprises

■ Un risque évident qui impose une protection adaptée

On ne peut imaginer que la gestion individuelle et collective du personnel (envisagée à travers toutes les finalités possibles, en partant des plus simples et anodines en allant vers les plus sophistiquées et perfides pour les droits et libertés des salariés), puisse se passer de l'usage 'un fichier de données personnelles.
Ainsi, la loi du 6 janvier 1978 apparaît comme un point de passage obligatoire dans la vie de l'entreprise, dans les rapports employeurs-employés.
Il en va d'ailleurs de même pour ceux établis entre les employeurs, les syndicats et les représentants du personnel. Ainsi, dans un arrêt du 6 avril 2004, la Cour de cassation a estimé que « *pour l'accomplissement de leur mission légale et la préservation de la confidentialité qui s'y attache, les salariés investis d'un mandat électif ou syndical dans l'entreprise doivent pouvoir y disposer d'un matériel ou procédé excluant l'interception de leurs communications téléphoniques et l'identification de leurs correspondants* ».

C'est sans nul doute le rapport rédigé en 1992 par le Professeur G. Lyon-Caen, intitulé « *Les libertés publiques et l'emploi* » commandé par le Ministre du Travail et de l'Emploi qui constitue le socle initial entre le droit de la protection des données personnelles et le droit du travail.
Ce rapport a fortement influencé le législateur lors de l'élaboration de la loi n° 92-1446 du 31 décembre 1992, à l'origine de l'article L 120-2 du code du travail :
« *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.* »
La loi de 1992 dans son article L 432-2-1, alinéa 2, fait également obligation d'informer le comité d'entreprise, préalablement l'introduction dans l'entreprise, des traitements automatisés de gestion du personnel et sur toute modification de ceux-ci. Aux principes de finalité et de proportionnalité s'ajoute donc le principe de transparence à travers une obligation d'information préalable.
Il en va de même pour tout ce qui concerne la gestion classique, administrative, financière, sociale du personnel, pour la gestion moderne des ressources humaines, l'évaluation qualitative et quantitative des capacités et comportements, la surveillance des employés au travail, la gestion du personnel passe obligatoirement par le traitement de données personnelles pour des finalités variées dont certaines peuvent présenter des risques pour les droits et libertés des employés. On peut ainsi citer la cyber surveillance, l'accès par l'employeur à la messagerie électronique, à l'ordinateur du salarié, la surveillance des usages des services liés à Internet, les contrôles d'accès aux locaux, du temps et de la qualité du travail, la traçabilité des données GPS ou du téléphone fixe ou mobile etc.…

A cela s'ajoute un ensemble de règles protégeant les employés. En effet, chaque salarié dispose d'un droit à la curiosité pour savoir si des données le concernant sont traitées, du droit de connaître les finalités du traitement, la nature des données traitées, les destinataires, du droit d'accéder aux données personnelles, de connaître leur origine et d'obtenir une copie (article 39), le droit de contester et d'obtenir effacement ou modification, avec un renversement de la charge de la preuve au détriment de l'employeur responsable du traitement (article 40). L'article 38 de la loi modifiée conserve un droit d'opposition à un traitement pour des motifs légitimes, l'article 7 posant le principe du consentement informé et éclairé au traitement de la personne concernée, principe qui connaît des exceptions et des aménagements dont l'interprétation peut soulever de multiples problèmes entre employeurs et employés.

Le responsable du traitement doit respecter les conditions de licéité précisées par le chapitre II de la loi modifiée : les données doivent être collectées et traitées de manière loyale et licites pour des finalités déterminées, explicites et légitimes, les données traitées doivent être adéquates, pertinentes, non excessives par rapport aux finalités, mises à jour, exactes, complètes et conservées pour une durée liée à la finalité d'usage.
Le traitement de certaines données sensibles (origines raciales et ethniques, opinions politiques, philosophiques, religieuses, appartenance syndicale, données sur la santé et la vie sexuelle, données sur la vie privée) est interdit sauf exception dont le consentement de la personne concernée (article 8).
Le responsable du traitement, c'est-à-dire l'entreprise-employeur, doit fournir lors de la collecte des données de multiples informations énumérées par l'article 32 de la loi aux employés et doit assurer une obligation de sécurité préventive pour protéger les données traitées contre les atteintes venant de l'intérieur et de l'extérieur de l'entreprise (article 34).
Le responsable du traitement devra accomplir éventuellement des formalités déclaratives ou obtenir de la CNIL une autorisation avant de procéder à un traitement automatisé de données personnelles (chapitre IV de la loi modifiée).
En cas de préjudice, l'entreprise-employeur, ou un salarié responsable personnellement, peut engager sa responsabilité civile mais aussi sa responsabilité pénale. Le non respect des règles principales de la loi Informatique, fichiers et libertés constitue un ensemble d'infractions pénales lourdement réprimées (cinq ans de prison et 300 000 euros d'amende), spécialement par les articles 226-16 à 226-24 du code pénal.

Le correspondant à la protection des données personnelles (CPDP) ou correspondant informatique et libertés (CIL)
A l'évidence, l'instauration d'un régime dérogatoire bouleverse les mentalités. Alors que la CNIL assure depuis 25 ans un contrôle a priori des traitements mis en œuvre par les organismes publics, est ici créé un personnage permettant d'assurer en interne une mise en conformité des traitements, sans avoir à passer par l'autorité de contrôle.
Cette novation en matière de droit est issue de la directive 95/46 CE du 25 octobre 1995. Elle est également le résultat d'un constat : la CNIL est sur la voie du déclin. Sans être non plus totalement fataliste, on doit tout de même porter les remarques suivantes. Le budget de la CNIL a tendance à s'éroder et les effectifs ne sont plus suffisants au regard des nombreuses fonctions qui lui sont confiées. La concentration de la CNIL (uniquement présente à Paris) conjuguées à ces manques de moyens financiers et humains conduisent à l'idée de décentralisation. Le CIL apparaît alors comme la solution évidente !

La désignation du CIL est facultative et permet un allègement considérable des formalités de déclaration; elle constitue surtout un moyen efficace de veiller à la bonne application, dans l'organisme, de la loi Informatique et Libertés et donc à assurer le respect du droit fondamental à la protection des données personnelles.
Tous les responsables de traitements et de fichiers peuvent recourir à cette formule, qu'ils soient publics ou privés, qu'ils aient le statut d'associations, de collectivités locales ou de grandes administrations de l'Etat, qu'il s'agisse de PME-PMI ou d'entreprises multinationales.

<u>Les missions du correspondant</u> :
Dans les trois mois suivant sa désignation, le correspondant doit dresser une liste des traitements automatisés pour lesquels il a été désigné. Cette liste peut bien entendu être tenue de manière informatisée. Cette liste doit être mise à jour régulièrement et chaque salarié doit pouvoir la consulter.
Le correspondant est également chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi. Il veille ainsi à l'application de la loi Informatique et

Libertés aux traitements pour lesquels il a été désigné. A ce titre, il est obligatoirement consulté préalablement à la mise en œuvre des traitements. A cette fin, il peut faire toute recommandation au responsable des traitements.
Le correspondant reçoit aussi les réclamations et requêtes des personnes concernées par les traitements pour lesquels il a été désigné, s'assure de leur transmission aux services intéressés et leur apporte son conseil dans la réponse apportée au requérant. Il veille également au respect du droit d'accès et d'opposition et à l'information des personnes sur leurs droits.
A cet effet, il contribue à l'élaboration et à la bonne diffusion de notes d'information, d'affiches,… afin de diffuser une « culture Informatique et Libertés » au sein de l'organisme.
Le correspondant informe encore le responsable de traitement des manquements constatés et le conseille dans la réponse à apporter pour y remédier. Dans certains cas, lorsque cela se justifie réellement, il peut arriver que le correspondant saisisse la CNIL des difficultés qu'il rencontre dans l'exercice de ses missions (par exemple : absence de consultation du correspondant avant la mise en œuvre des traitements, impossibilité d'exercer ses fonctions du fait de l'insuffisance des moyens..., mais aussi difficultés d'application des dispositions législatives et réglementaires). Bien sûr, ceci ne sera possible qu'après que le correspondant ait effectué les démarches nécessaires auprès du responsable de traitements et que celles-ci soient demeurées infructueuses.

■ Les domaines touchés par ce risque dans l'entreprise

- Les opérations de recrutement
- Les annuaires du personnel
- L'accès au dossier professionnel
- La gestion des œuvres sociales et culturelles
- Les transferts internationaux de données
- Contrôle de l'utilisation d'internet et de la messagerie
- Les administrateurs réseau
- La vidéosurveillance sur les lieux de travail
- La gestion de la téléphonie
- Les dispositifs de géolocalisation GSM/GPS
- L'utilisation de badges sur le lieu de travail
- La biométrie sur le lieu de travail

La notion de protection des « données à caractère personnel » est étroitement liée à celle de données concernant la vie privée. Pour les juristes, le texte fondateur de la vie privée, qui a directement orienté l'exercice de ces droits, est, de l'avis unanime des commentateurs, un article paru dans la revue de droit de Harvard en 1890 et que l'on doit à l'encre mêlée d'un juriste de Boston et d'un homme d'affaires de New York. Sous le titre « Le droit à la vie privée », les deux auteurs y réclamaient le droit pour les personnages publics d' « être laissés seuls » (the right to be left alone), c'est-à-dire de ne pas être importunés dans leur intimité par les curiosités et les divulgations de la presse à sensation.

Depuis, la notion de vie privée et de protection des données personnelles a évolué et évolue encore.

Avec l'inauguration par le Ministre de l'immigration (*Eric BESSON*) du système PARAFES (passage automatisé rapide aux frontières extérieures Schengen) à l'aéroport de Roissy-Charles-de-Gaulle le 19 octobre 2009, on constate sans hésitation l'augmentation exponentielle du nombre de fichiers comportant des données à caractère personnel dans notre actualité.

Si des règles de droit sont établies au niveau national et européen comme nous avons pu le voir, il semble que la difficulté se situe plutôt au niveau de l'application et notamment de l'adaptation des mentalités à des activités relevant de l'immatériel et donc d'éléments n'ayant pas de corporalité.

En décembre 2008, la revue « *Le Tigre* » a parfaitement illustré, par une démonstration astucieuse, comment certains internautes ouvraient leur intimité au monde entier, sans avoir toujours mesuré la portée d'un tel acte sur leur vie privée.

Dans les entreprises, le problème se pose dans les mêmes termes. Les procédures faisant appel aux données à caractères personnel se multiplient rapidement et les écarts apparaissent nombreux (*voir notamment l'affaire « société Doubleclick » - 2002*).

Si l'Etat français a compris l'importance de l'économie de l'immatériel en créant en 2007 l'agence du patrimoine immatériel de l'Etat (suite au rapport Lévy-Jouyet), il semble qu'une réflexion importante doit être réalisée sur le travail pédagogique à mettre en œuvre notamment en direction des plus jeunes afin d'appréhender au mieux ces notions parfois mal appréciées.

SOURCES

► RAPPORT DE LA CNIL - RAPPORT - « *30 ANS : DE 1978 A 2008* »

► GUIDE DE LA CNIL - « *POUR LES EMPLOYEURS ET LES EMPLOYES* »

► GUIDE DE LA CNIL - « *LE CORRESPONDANT INFORMATIQUE ET LIBERTES* »

► Colloque - Paris Sud XI, Faculté Jean Monnet, Sceaux - 14 décembre 2007 sur « *La protection des données personnelles : Une perspective juridique* » ; **Anne-Catherine Lorrain (CERDI - Centre d'Etudes et de Recherche en Droit de l'Immatériel - Universités Paris I Sorbonne – Paris Sud XI)**

► « Internet et la protection de la vie privée » : Louise Cadoux et Pierre Tabatoni

► LA REGULATION DES DONNEES PERSONNELLES, n°42 de la revue Légicom, édité par Victoires Editions, avril 2009, collectif. Sommaire (extrait) : La CNIL :missions et sanctions - Le Groupe Article 29 - Le Correspondant Informatique et Libertés - La question de l'adresse IP - Les données personnelles des salariés - La régulation économique des données personnelles, etc. Plusieurs de ces articles sont signés de membres AFCDP.

►Informatique et libertés mode d'emploi - Cybersurveillance, déclarations CNIL, correspondant informatique et libertés, NTIC et ressources humaines

Rédaction de La Revue Fiduciaire

Editeur : Groupe Revue Fiduciaire - **Collection :** Les essentiels RF

ISBN : 978-2-7579-0067-3 - 234 pages - Parution : 06/2007

Présentation par l'éditeur

Cet ouvrage vous présente en 115 mots-clés tous les aspects relatifs au respect de la vie privée et des libertés individuelles des salariés dans l'entreprise. Il expose les règles à connaître et la marche à suivre dans l'utilisation des nouvelles technologies de l'information et de la communication dans l'entreprise comme mode de surveillance des salariés ou encore comme outil de gestion des ressources humaines. Faut-il saisir la CNIL et comment ? L'entreprise a-t-elle intérêt à désigner un correspondant informatique et libertés ? Cet ouvrage apporte toutes les réponses concrètes.

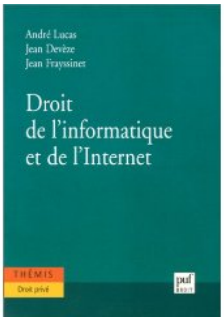
►Protection des données à caractère personnel - *Tout sur la nouvelle loi*

Marie-Laure LAFFAIRE
février 2005

- Principes généraux
- Champ d'application
- Finalité du traitement et notion de licéité du traitement introduite par la nouvelle loi
- Les différents intervenants
- La collecte de données à caractère personnel
- Les droits des personnes concernées
- Accomplissement des formalités auprès de la CNIL
- Les obligations incombant au responsable du traitement
- Le transfert à l'étranger de données à caractère personnel
- Les opérations et les traitements particuliers
- Les contrats
- Les missions et pouvoir de la CNIL
- Les sanctions
- Panorama européen

► Droit du travail et nouvelles technologies. Collectes des données, Internet, Cybersurveillance, Télétravail (Broché) de Isabelle de Benalcazar (Auteur)

-
- Broché: 260 pages
- Editeur : Gualino Editeur (28 février 2003)
- Collection : Business
- Langue : Français
- ISBN-10: 2842006453
- ISBN-13: 978-2842006457



Droit de l'informatique et de l'Internet (Broché)
de André Lucas (Auteur), Jean Devèze (Auteur), Jean Frayssinet (Auteur)
Broché: 748 pages
Editeur : Presses Universitaires de France - (6 nov 2001)
Collection : Themis
Langue : Français
ISBN-10: 2130518222
ISBN-13: 978-2130518228

► **Le droit du travail à l'épreuve des NTIC**. Par Jean-Emmanuel Ray, Editions Liaisons, Date de parution : novembre 2001 (2ème édition), ISBN 2.87880.422.3

► « informatique, fichiers et libertés » : M. Jean Frayssinet. 1992. Litec

► "La protection pénale de la vie privée" : Levasseur. Mélanges Kayser T2. p.107

► "La protection pénale de la vie privée" Roger Nerson et Jacqueline Rubellin-Devichi. RTDC 1983. p.103

► "informatique et liberté en 1997 : vers où allons nous?". Louise Cadoux Gaz. Pal - 1997 I Doctrine p.642

► "Secret professionnel, confidentialité et nouvelles technologies d'informations" : Philippe Lafarge. Gaz. Pal. 1998 (1er sem.)

► "La loi du 1er juillet 1994 relative au traitement des données nominatives" : M. Jean Frayssinet et M. Philippe Pedrot. JCP 1994 n°3810

► "Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques" - M. Jean Frayssinet. Editions du Juris-Classeur (pénal)

► "Le secret professionnel" : André Damien. Gaz. Pal. 16 mars 1982. Doctrine 136

► "La C.N.I.L et la protection de la vie privée" : Sophie Vulliet-Tavernier. Gaz. Pal. 5 Août 1999