GUIDE D'ELABORATION
d'une CHARTE D'UTILISATION
des MOYENS INTRANET ET INTERNET

Avril 2002
Version 1.0

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS

30 rue Pierre Semard, 75009 PARIS
Tél : +33 153 25 08 80 – Fax : +33 1 53 25 08 88 – email : clusif@clusif.asso.fr
Web : http://www.clusif.asso.fr

Remerciements

Sous l'impulsion de Pierre SINOQUET, Président de l'Espace RSSI, et Denis LEFEUVRE, Coordinateur des Travaux du CLUSIF, ce document a été réalisé dans un contexte législatif et sécuritaire très mouvementé en 2001, notamment dans les conséquences sur la vie économique des diverses jurisprudences et lois sur la sécurité.

Nous tenons donc à souligner la contribution importante des membres de l'Espace RSSI à la production de ce document unique en France :

Jean-Pierre CAZAUX ROCHER	GROUPE MALAKOFF
Gérard COUTANT	G.I.E. HENNER
Marie-Agnès COUWEZ	CLUSIF
Paul GRASSART	CLUSIF
Albert GUILIANO	MINISTERE DE LA DEFENSE
Denis LEFEUVRE	PREDICA
Patrick MERY	CNAV - DSINDS
Jean-Laurent SANTONI	MARSH CONSEIL
Constanza SEMILLA	CLUSIF
Pierre SINOQUET	MAIRIE D'AMIENS
Régine WAGNER	MAIRIE DE PARIS

Nous tenons également à remercier la Commission Nationale Informatique et Libertés, et en particulier Madame Sandrine MATHON, pour les précisions juridiques qu'elle nous a apportées.

Table des matières

Avertissement

Ce document a pour objectif d'aider à l'élaboration d'une charte d'utilisation des moyens Intranet et Internet en entreprise. Il est conçu davantage comme une « boîte à outils » pour le RSSI que comme une charte-type prête à l'emploi.

En effet, deux éléments clés doivent rester présents à l'esprit du lecteur afin de tirer le meilleur bénéfice de ce guide :

1. Avec l'usage massif des techniques Internet dans l'environnement économique, la législation applicable est en pleine évolution. Les échanges économiques européens et internationaux, le commerce BtoC transfrontalier génèrent une évolution parallèle des législations concernées.

2. Selon la législation du travail actuellement applicable en France, la culture d'entreprise est un élément incontournable[1] à prendre en compte dans l'élaboration d'une charte de ce type.

Nous envisageons de remettre ce guide périodiquement à jour en fonction des évolutions juridiques, telles que lois, décrets et jurisprudences, qui impacteront significativement sur le fonctionnement de l'entreprise.

[1] Cet axe social est amplement recommandé par la CNIL (2001).

Partie 1 : La problématique

L'objectif immédiat d'une telle charte d'utilisation est de fournir à tous les intervenants de l'entreprise un support définissant les bonnes pratiques comportementales en entreprise :

- comportement loyal et responsable,
- règles élémentaires de sécurité,
- règles déontologiques et législations générales applicables.

Ces points se déclineront par rapport aux activités classiques effectuées depuis un poste de travail informatisé et connecté au réseau de l'entreprise.

Les bonnes pratiques donneront un cadre de référence et non un périmètre défini et précis, pour utiliser au mieux les outils informatiques que sont la messagerie, le Web et de façon générale tous les outils d'échange numérique.

La charte sera une synthèse entre le respect de la Loi par l'entreprise et par les salariés, les exigences de protection des intérêts vitaux de l'entreprise et les besoins personnels fondamentaux du salarié à l'intérieur de l'entreprise.

1. Potentiels des nouvelles technologies de l'information et de la communication (NTIC)

L'objet de ce chapitre est d'éclairer le lecteur sur les potentialités de contrôles fournies en standard par les NTIC.

1.1. Possibilités de traces offertes par la technologie

La mise en œuvre de l'informatique s'est toujours accompagnée de la création de fichiers "traces", constitués de l'enregistrement automatique et systématique des actions informatiques élémentaires effectuées par les systèmes, sous-systèmes et logiciels lors de leur fonctionnement.

L'évolution des technologies a amplifié ce phénomène, et aujourd'hui les traces peuvent se scinder en trois catégories :

- Pour le fonctionnement du système et des logiciels eux-mêmes, à titre préventif ou curatif : détecter les pannes, améliorer les performances.
- Pour la sécurité des données de l'entreprise : maîtriser les autorisations d'accès, suivre et contrôler l'activité.
- Pour que l'entreprise et ses dirigeants puissent assumer correctement leurs responsabilités : restreindre par filtrage certains accès ou actions, considérés comme étant hors du champ professionnel de l'entreprise.

1.2. De l'usage technique des traces

La prise de traces peut être obligatoire, recommandée, facultative, ponctuelle, selon les traitements ou le but recherchés.

Le revers de la médaille est que ces traces, appelées aussi fichiers de journalisation ou fichiers « logs », constituent de fait un élément permanent de cyber-surveillance de l'activité des utilisateurs. Elles enregistrent à tout instant « qui fait quoi, quand et comment », sans que les utilisateurs en aient forcément conscience.

Sans entrer dans les détails techniques, les quelques exemples de "logs" ci-après illustrent cette situation.

1.2.1. Au niveau applicatif :

Les logiciels de gestion du travail de groupe, ou workflow, imposent l'enregistrement permanent pour établir la circulation des documents entre les acteurs du groupe. Le fichier « logs » ainsi constitué permet de :

- contrôler et suivre l'avancement d'un dossier donné,
- constituer le fichier historique qui pourra être potentiellement exploité à n'importe quelle fin, y compris un contrôle de productivité individuelle.

Dans d'autres cas, la trace est constituée à des fins de preuve (passage d'ordres de bourse), ou pour un besoin pédagogique (télé-vendeurs dans un centre d'appel). Il est clair que le contenu du fichier « logs » permet d'établir l'activité détaillée, exhaustive et datée des utilisateurs.

1.2.2. Moniteurs de télétraitement et SGBD/R

Les moniteurs de télétraitement (exemple CICS) et les gestionnaires de bases de données (exemple DB2, Oracle) utilisent les techniques de fichiers ou « logs » afin de ne pas perdre les dernières transactions des utilisateurs en cas d'incident.

Ce dispositif contribue à l'intégrité des fichiers et des applications associées. Il enregistre en permanence toutes les données qui ont fait passer un système applicatif d'un état stable à un autre (quelles données et suivant quels éléments chronologiques).

1.2.3. Réseaux informatiques

La surveillance du réseau informatique permet de détecter les pannes, de déceler les engorgements, de répartir les charges.

Elle consiste également à utiliser des sondes placées aux points sensibles. L'analyse des données est ensuite effectuée soit en temps réel (détection d'intrusion), soit en différé (analyse d'activités).

Généralement un logiciel spécialisé réalise en continue la collecte des informations élémentaires des échanges dans un fichier « logs ».

Ces outils qui mesurent les débits, surveillent certains matériels (routeurs, pare-feux), comptabilisent le nombre et la durée des appels, permettent également de savoir quelle personne est connectée, quelle est ou a été son activité en reconstituant le chemin parcouru.

En cas d'incident, l'examen du fichier « logs » permet de dérouler le fil des opérations et d'aider à la compréhension du problème.

1.2.4. Télémaintenance

Les techniques de télémaintenance et les outils de prise de main à distance sont souvent utilisés pour la gestion d'un parc de terminaux important ou géographiquement dispersé, ainsi que pour la détection des pannes et leur correction.

Ces logiciels permettent de suivre en temps réel tous les faits et gestes d'un usager distant, ou d'avoir accès aux fichiers disponibles sur son disque local.

1.2.5. Firewalls

La mise en place d'une fonction pare-feu (firewall) répond au besoin de protection des réseaux internes des entreprises contre les attaques extérieures issues d'Internet, ainsi qu'au filtrage des communications, à l'authentification des personnes qui se connectent, au chiffrement et au contrôle des accès utilisateurs entrants ou sortants.

Cette fonction, reposant sur des produits logiciels et/ou matériels, collecte et analyse une énorme masse de données.

Si elle est le meilleur gardien de l'entreprise de par sa nature, elle peut devenir son meilleur « espion », dans la mesure où elle détient toutes les traces de l'activité qui transite obligatoirement sous son contrôle (navigation sur Internet, envoi et réception de mails).

1.2.6. Proxy

Les fonctions de serveur proxy permettent, en mémorisant les pages web consultées par les internautes, d'optimiser les temps de connexion en retrouvant rapidement une page précédente dans un espace disque proche de l'utilisateur.

Cette fonction de mémorisation des pages permet techniquement à une entreprise de surveiller l'utilisation d'Internet par ses salariés et autres intervenants.

1.2.7. Messageries

La création d'une adresse électronique nécessite l'utilisation des services de serveurs de messageries. Lorsqu'un internaute émet ou reçoit un message, une trace en est conservée sur le disque de son ordinateur et sur divers composants du réseau utilisé.

D'autre part le serveur de messagerie prend lui-aussi une trace du mail entrant ou sortant. Il est tout à fait possible, directement ou via des outils spécialisés d'analyse du contenu des messages, d'accéder à ces différents niveaux de traces et de prendre connaissance de l'identité des auteurs et de la nature de leurs échanges.

1.2.8. Navigation Web

La navigation sur Internet (web) s'accompagne souvent, à des fins de performance, d'enregistrements sur le disque dur de l'internaute à trois niveaux : en mémoire cache des pages accédées (temporary Internet files), dans le fichier historique des consultations Internet (adresses ou URL), et via l'écriture de cookies (petits fichiers texte).

Effectués plus ou moins discrètement, ils sont révélateurs de l'activité de l'internaute. Les cookies permettent de plus d'établir un comportement type de l'internaute.

2. Les droits fondamentaux du salarié

Dans ce chapitre, nous proposons une synthèse sur les droits fondamentaux du salarié en matière de vie privée en environnement professionnel.

2.1. La problématique

Les nouvelles technologies de l'information, de part leur facilité de mise en œuvre sont devenues un moyen de communication en entreprise, et à moindre titre dans les foyers, à l'instar de la lettre ou du téléphone.

Si les facilités de communications personnelles, accordées ou tolérées jusqu'ici en entreprise peuvent, de principe, également s'appliquer à ces nouveaux moyens, il apparaît néanmoins un changement très important dans les conséquences de l'utilisation de ceux-ci.

En effet, l'extrême rapidité des échanges électroniques favorise une accélération des volumétries échangées. Le fait que ces nouveaux outils soient bien intégrés dans le poste de travail génère légitimement trois craintes majeures chez les responsables d'entreprise :

- La fuite matérialisée d'informations plus ou moins sensibles lors des échanges personnels ;
- Une contre-productivité préjudiciable au bon fonctionnement de l'entreprise, soit par une distraction importante du temps de travail au profit d'échanges personnels, soit par une obligation d'accroître la puissance et la capacité des moyens informatiques ;
- La complicité, même involontaire, et l'infraction pénale ;

L'objet de cette partie est de présenter, le plus complètement possible, ce que nous désignons généralement par « vie privée résiduelle en entreprise ». A partir des raisons objectives qui ont fait naître cette appellation, comment cette « vie privée » peut s'exprimer avec les nouveaux moyens de communication ?

2.2. La nécessité de disposer d'une « vie privée résiduelle » en entreprise

L'existence d'une vie privée dans l'entreprise s'explique au premier chef par le besoin d'équilibre psychologique du salarié.

En effet, en moins d'un demi-siècle, le fonctionnement de la vie économique a profondément évolué. Malgré une baisse constante du temps de travail, les bénéfices ou les bienfaits attendus ne sont pas toujours au rendez-vous.

A titre d'illustration, nous citerons quelques-unes de ces évolutions qui nécessitent, voire imposent, une vie privée résiduelle en entreprise :

- La taille de l'unité familiale est très majoritairement réduite au couple avec ses enfants et nous notons que la famille mono-parentale devient un fait de société incontournable. En contre-partie, nous voyons que les ascendants, lorsqu'ils deviennent dépendants, doivent être souvent pris en charge par des solutions externes[2] à la famille.

[2] Les compagnies d'assurance vie ont lancé récemment les premiers contrats d'assurance Dépendance.

- Indépendamment de l'amélioration de la condition féminine, la capacité financière des ménages impose le salariat aux deux parents, ce qui implique une solution externe de garde d'enfants (crèches, activités encadrées, internat, baby-sitting, etc.).
- L'organisation et l'implantation géographique des sociétés peuvent allonger artificiellement le temps de travail par les temps de transports ou des missions « longues distances »..

Ces trois points montrent aisément que le salarié a besoin de conserver un lien de communication immédiat avec ses proches, même virtuel.

2.3. L'environnement familial

L'environnement familial, tel qu'esquissé précédemment, implique que le salarié puisse être joint à tout moment en cas de problème d'un membre proche de sa famille, notamment pour exprimer et exercer sa responsabilité parentale à l'égard de tiers (écoles, crèches, etc.).

Que ce soit pour des raisons touchant au domaine de la santé ou pour la protection des enfants, le média téléphonique s'est révélé un moyen évident par sa facilité d'usage et sa rapidité intrinsèque pour joindre une personne.

D'autre part, le temps privé hors entreprise peut être réduit de façon si importante que le salarié ne puisse plus assumer son rôle obligatoire d'assistance, (« non-abandon ») de ses propres parents par exemple. Là aussi la communication par téléphone pendant les plages horaires adéquates est le moyen le plus facile.

Dans la mesure où ces quelques conditions de vie ne changent pas dans des proportions importantes et généralisées, il est certain que tout nouveau moyen technologique qui apporte des facilités similaires ou plus grandes que le téléphone sera naturellement utilisé.

2.4. Réciprocité entreprise et salarié : l'échange de bons procédés

S'il apparaît qu'un salarié absent pour cause de maladie représente un certain coût pour la collectivité, il n'en demeure pas moins que l'absentéisme sous toutes ses formes pénalise sérieusement le fonctionnement de l'entreprise.

Au-delà de la santé physique, il devient évident qu'il est de l'intérêt de l'entreprise d'offrir des conditions de travail décentes pour que les simples soucis de ses salariés ne génèrent pas un stress improductif, ou dans le pire des cas, un facteur de dégradation du climat social.

Cet aspect est institutionnalisé avec le CHSCT (Comité d'Hygiène, de Sécurité et des conditions de Travail - art L.262), entité représentative du personnel, qui est doté de pouvoirs délibératifs non seulement pour les questions de santé et de sécurité mais aussi de qualité de vie au travail.

La mise à disposition par l'entreprise de moyens pour satisfaire les besoins privés de ses salariés va encore plus loin dans certains secteurs économiques. En effet, des sociétés dont le principal capital est la matière grise, n'hésitent pas à créer des points d'accueil "laverie", "crèche", "contacts administratifs".

Délivré de ces contraintes matérielles, le salarié gagne autant que l'entreprise en temps de travail effectif et efficace.

En contre partie, les nouveaux moyens de communication permettent au salarié d'entretenir et d'augmenter son savoir et son « savoir-faire » grâce aux échanges avec des homologues travaillant hors de son entreprise. Ces échanges sont de l'intérêt de l'entreprise, d'autant que cette approche reflète une forte implication personnelle. L'entreprise commence à utiliser les possibilités de cette démarche avec le e-learning.

Il devient alors évident que l'octroi naturel d'un espace privé résiduel en entreprise est un avantage qualitatif certain et partiellement mesurable pour les deux parties.

2.5. Matérialisation de cet espace de vie privée résiduelle

Si le terme « résiduel » est utilisé cela signifie qu'il ne doit pas y avoir d'ambiguïté dans les rapports « temps de travail » et « temps privé ».

La législation française et le contrat de travail référencent contractuellement une quantité de temps qui doit être fourni. Il ne serait pas concevable qu'un pourcentage significatif vienne en déduction de ce temps.

Mais alors, comment matérialiser un « temps résiduel » qui n'a pas de périmètre précis ?

Les pistes suggérées s'appuient sur le fonctionnement usuel de quelques activités, notamment dans les secteurs où les salariés disposent d'un poste de travail hautement informatisé mais sans que cela soit un travail « posté » (type "hot line", "télévendeur", etc.).

2.5.1. Encadrement de l'espace de vie privée : règlements internes et bons usages

Généralement, les règles internes de l'entreprise évoquent de façon plus ou moins précise les limites et tolérances accordées aux salariés quant aux aspects de communications personnelles : courrier traditionnel ou téléphonie.

Ces règles peuvent être exprimées sous différentes formes : règlement intérieur, charte d'utilisation des moyens informatiques, notes de direction, guide d'accueil du personnel, etc.

La teneur de ces documents ne peut en aucun cas être plus restrictive que les textes légaux et doit faire explicitement référence aux tolérances « vie privée », notamment pour certaines causes d'absentéisme.

2.5.2. Temps personnel

Si le législateur n'a pas quantifié ce temps, nous essaierons d'approcher le problème par les temps improductifs naturels que sont, par exemple, les pauses « café », moment d'échange avec les collègues.

Ces temps soustraits au travail productif s'ajoutent à l'estimation des charges de travail.

Dans le même esprit d'ouverture et de raison, il est nécessaire d'octroyer un temps similaire et proportionnel aux autres formes de communication personnelle.

En revanche, il ne faut pas basculer dans l'excès qui consisterait à cumuler mécaniquement tous ces temps personnels. Le verdict serait immédiat : les métriques verraient une chute de leur

valeur utilisée et, à défaut de sanction managériale pour un travail non terminé dans un temps négocié, l'entreprise accuserait une contre-productivité.

2.5.3. Communications personnelles

La vie privée en environnement professionnel est également matérialisée par les procédures d'utilisation des moyens de communication électronique.

L'existence d'une adresse « email » et d'un système de messagerie ouvert sur l'extérieur offrent de facto toutes les possibilités inhérentes à ce média.

Toute restriction ou encadrement d'usages personnels doit faire l'objet d'une information aux salariés et de procédures automatisées supportant le fonctionnement encadré. Dans la négative, le salarié pourrait se prévaloir d'une erreur involontaire dans la mesure où aucun dispositif ne l'aurait alerté de son « oubli ».

A noter également que l'existence et l'usage (encadré ou non) des marqueurs spéciaux de messagerie (confidentiel, privé, etc.) et d'un carnet d'adresses personnelles matérialisent une nouvelle fois l'espace de vie privée en entreprise.

2.5.4. Espaces électroniques personnels

L'organisation des espaces disques sur les serveurs du réseau local d'entreprise est aussi une approche pour matérialiser l'espace de vie privé.

De façon plus ou moins normalisée ou organisée, la destination des espaces disques personnels (disque local sur poste de travail, présence d'un lecteur de disquette ou autre support amovible, voire même un espace sur disque serveur) et l'existence ou non d'une classification des informations, matérialisent aussi les possibilités laissées à la discrétion du salarié.

A noter que l'existence de telles possibilités doivent au minimum faire l'objet d'une communication sur les obligations légales du salarié : respect des droits et licences, respect de la législation concernant le respect d'autrui et surtout être loyal envers l'entreprise (ne pas exercer une activité de nature concurrentielle par exemple).

3. La prise de position publique du Clusif

Le contenu de ce chapitre est la copie intégrale de la prise de position du CLUSIF lors de la consultation publique lancée par la CNIL en juin 2001, sur le thème de « la cyber-surveillance des salariés ».

Les entreprises doivent garder les moyens de faire respecter la loi

La Commission Nationale Informatique et Libertés a lancé une consultation publique sur la « cyber-surveillance » des salariés dans l'entreprise, matérialisée par le rapport d'étude proposé sur son site. Elle y pose quatre questions :

1. Les technologies en réseau sont-elles différentes des technologies précédentes ?
2. Y a-t-il une vie privée résiduelle du salarié dans l'entreprise ?
3. Quel usage à des fins privées des outils mis à disposition des salariés ?
4. Quelles sont les limites à la surveillance des salariés ?

Le CLUSIF (Club de la Sécurité des Systèmes d'Information Français) estime que si la CNIL rappelle bien le cadre juridique et indique quelques bonnes pratiques, il demeure nombre de lacunes par rapport à la réalité, qui interpellent le CLUSIF quant à la finalité du document et de la consultation lancée par la CNIL.

Au-delà d'une multitude d'aspects positifs : les possibilités offertes par les réseaux - et plus généralement ce qu'on appelle les T.I.C.-, d'une part, et la nécessaire et inévitable interconnexion des systèmes d'information des entreprises, d'autre part, ont pour effet immédiat de rendre les systèmes d'information très vulnérables, tant **en raison de la convergence totale entre « hacking » et infections informatiques, que de la dispersion géographique de tous les utilisateurs possibles.**

Sans multiplier les exemples, on peut ainsi évoquer celui des infections informatiques (tels que les virus, les vers, etc.) qui, introduits dans l'entreprise par le biais des messageries (directes ou utilisées par des solutions de type CRM), peuvent ensuite constituer autant d'accès illicites aux systèmes d'information d'une entreprise et mettre alors en danger ses données voire son activité complète.

Par ailleurs, en cas d'accès illicite à des données nominatives, la responsabilité pénale de l'entreprise elle-même et de ses cadres peut être engagée, l'article 226-17 du Code Pénal fixant en effet une **obligation de résultat** quant à la sécurité de ces informations.

Dans ce contexte, si l'on admet volontiers que l'octroi naturel d'un espace privé résiduel en entreprise est un avantage qualitatif certain, et même partiellement mesurable par l'employeur et le salarié, on ne peut faire l'impasse sur la mise en place de sécurités. Ces moyens de contrôle n'ont qu'une finalité : protéger le patrimoine informationnel de l'entreprise, son activité et son personnel tout en respectant les lois en vigueur.

Dans le même esprit, outre les droits, les devoirs et les obligations des utilisateurs devraient pouvoir être clairement définis et intégrés sous une forme directe ou indirecte au contrat de travail.

Les outils de surveillance n'ont pas d'autre but que de détecter les actions potentiellement dommageables pour l'entreprise et son système d'information. Toute autre finalité procéderait d'une certaine dérive.

Si l'on se rapporte - par comparaison - à la « norme simplifiée n° 40 » qui avait été défini par la CNIL pour les autocommutateurs téléphoniques, celle-ci constitue un exemple **d'équilibre entre les possibilités de recueil d'informations par l'entreprise et la protection des salariés**. A contrario de ce texte qui pourrait être une base de réflexion intéressante, la tonalité générale du rapport d'étude ne laisse-t-elle pas entrevoir une certaine inflexion, voire une régression dans la doctrine de la Commission ?

Enfin, concernant l'exploitation éventuelle des fichiers associés à ces outils de surveillance, se pose avec acuité la question du statut réel et reconnu des administrateurs des systèmes informatiques et des responsables sécurité, et de leur protection contre d'éventuelles dérives dans le cadre de leur responsabilité. Comment leur donner les moyens de s'opposer au détournement de finalité d'un système de contrôle, par ailleurs régulièrement déclaré à la CNIL ?

En conclusion, l'affirmation de la notion de « vie privée résiduelle » ne peut se faire isolément : elle doit impérativement s'inscrire dans le contexte légal complet, à savoir :

- Les droits et les obligations du salarié ;
- Les obligations légales auxquelles l'entreprise doit répondre ;
- Les moyens de protection légaux que l'entreprise doit garder pour assurer sa pérennité, assumer ses responsabilités et faire respecter la loi.

Pourquoi une charte d'utilisation des moyens Intranet et Internet ?

Etablir une telle charte d'entreprise correspond à la prise de conscience de l'accroissement des risques liés aux NTIC et à la volonté de clarifier l'approche pratique pour les circonvenir au mieux, dans l'intérêt de l'entreprise et de ses salariés.

Cette charte trouvera donc son expression et sa finalité entre les bases légales et ses propres fondamentaux lui permettant d'assurer et d'assumer son activité et ses engagements.

4. Les fondamentaux

4.1. Les périmètres fondamentaux d'une charte d'utilisation

Via la formulation usuelle d'encadrement de « l'usage des moyens de communication sur les lieux de travail », la véritable problématique ciblée par une charte de sécurité d'entreprise peut se résumer aux trois points suivants :

- La preuve (par exemple : les fichiers « logs ») de l'usage qui est fait des moyens de l'entreprise ;
- Le contenu des échanges directs ;
- Les échanges indirects, notamment les forums, qui ciblent les problèmes liés à l'intelligence économique.

4.2. Charte et enjeux d'une politique de sécurité

A ce jour, aucun processus de surveillance électronique de l'activité des salariés ne peut être mis en œuvre sans appliquer les dispositions préalables prévues par la législation française.

Ainsi, l'entreprise doit avertir les organisations représentatives du personnel. Cette disposition peut entraîner une modification du climat social, une répercussion négative sur le fonctionnement interne ou affecter l'image externe (cf. contre-sites de salariés ou sites externes spécialisés dans le recueil « d'humeurs » des salariés).

Sur la base de principes de sécurité clairs et justifiés, la politique de sécurité générale de l'entreprise représente donc un fondement important dans l'établissement du climat social et de la culture d'entreprise.

A défaut de supprimer les craintes légitimes des salariés, les modes d'élaboration, de diffusion et de communication de la politique de sécurité générale permettront à chaque salarié d'appréhender la problématique sécuritaire de l'entreprise et de percevoir clairement les droits et devoirs de tous les acteurs concernés.

Si la finalité majeure d'une politique de sécurité générale est de garantir les services rendus par l'entreprise ainsi que la protection des biens et des informations, les modalités pratiques se déclinent autour de l'ensemble du personnel œuvrant au sein de la société.

Pour illustrer le propos, nous citerons les deux objectifs majeurs usuellement retenus :

- Fournir un cadre général pour aider les personnes chargées d'élaborer et de mettre en œuvre les procédures de sécurité ;
- Donner à tout le personnel les règles et les moyens pour bien utiliser les systèmes d'information ;

La « cyber-surveillance » des salariés est donc l'une des mesures préventives qui sera mise en œuvre et expliquée suivant les principes retenus par l'entreprise dans sa politique de sécurité générale.

Si la malveillance s'exerce aussi bien de l'extérieur que de l'intérieur de l'entreprise, nous ne retiendrons que la problématique interne dans le cadre de notre étude.

La nécessité d'une sécurité du personnel par la mise en œuvre d'une cyber-surveillance s'explique principalement par les objectifs suivants :

- Protéger l'entreprise de la fuite de ses informations ;
- Dissuader d'une certaine malveillance ;
- Susciter la rigueur pour éviter les risques liés à la négligence.

Dans ce contexte, les enjeux et la promotion d'une politique de sécurité générale passent par l'information et la sensibilisation du personnel en matière de risques et menaces encourus par l'entreprise et ses salariés. Des dispositifs de cyber-surveillance, déclinés dans la politique de sécurité, n'ont pour vocation que de matérialiser un code commun de bonne conduite auquel chaque salarié pourra se référer et s'auto-contrôler.

5. Les bases légales

Appliquer la loi en vigueur peut se schématiser comme suit :

5.1 Protéger la vie privée

Ce principe est posé par différents textes :
- Au plan général par l'article 8 de la Convention européenne des Droits de l'Homme ;
- Par l'article 9 du Code Civil ;
- Par l'article 226-22 du Code Pénal, qui assimile la divulgation des informations portant atteinte à la vie privée à un délit, punissable d'un an de prison et 15.245 € (100 000 F) d'amende. Dans ce dernier cas, l'entreprise peut être déclarée civilement responsable (cf. art. 1384 du Code Civil).

5.2 Protéger les autres droits des personnes

Obligation	***Fondement légal***	SANCTIONS EN CAS DE MANQUEMENT	
		personnes physiques	***personnes morales***
- **Protéger les personnes**			
	Loi " Informatique et Libertés " du 6-1-78 et Code Pénal		Sanctions prévues par les articles 131-38 et 131-39 du Code pénal: <u>Pour toutes les infractions, en général :</u>
- déclaration à la C.N.I.L.	- L. art. 15 et 16 / CP art. 226-15	5 ans, 2 M.F.	▪ Amende appliquée pour les personnes physiques <u>multipliée par 5.</u> ▪ <u>Peines complémentaires</u> pouvant aller de la publication du jugement par tous moyens de presse, à la confiscation du matériel, jusqu'à la fermeture définitive de l'entreprise
- droit de s'opposer au traitement	- L. art. 26 / CP art. 226-18	5 ans, 2 M.F.	
- ne pas détourner la finalité du traitement	- L. art.19 / CP art. 226-21	5 ans, 2 M.F.	
- ne pas conserver les informations nominatives au-delà de la durée nécessaire	- L art. 28 / C.P. art. 226-20	3 ans, 300 K.F.	
- obligation de sécurité	- L. art. 29 / C.P. art. 226-17	5 ans, 2 M.F.	
- ne pas recourir à des moyens déloyaux ou illicites	- L. art. 25 / C.P. art. 226-18	5 ans, 2 M.F .	Les informations à caractère nominatif ainsi recueillies de façon irrégulière seront en outre juridiquement inexploitables (par ex. : contentieux prud'hommal)
- ne pas divulguer des informations portant atteinte à la vie privée	- C.P. art.226-22	1 an, 100 K.F.	Dommages et intérêts versés par l'entreprise, celle-ci étant responsable (Code Civil art. 1384)

Obligation	*Fondement légal*	SANCTIONS EN CAS DE MANQUEMENT	
		personnes physiques	*personnes morales*
PROTEGER LES LOGICIELS ET LES DONNEES (EN TANT QU'ŒUVRES ORIGINALES)			
	Code de la Propriété Intellectuelle : L 335-1 à L335-8	2 ans, 1 M.F.	Amende 5 M.F. Peines complémentaires (cf. ci-dessus).
PROTEGER LES BASES DE DONNEES			
	Code de la Propriété Intellectuelle L342-1 à L 342-5, et L 343-1, L 343-2	2 ans, 1 M.F.	Amende 5 M.F. Peines complémentaires (cf. ci-dessus).
PROTEGER LES INFORMATIONS CONFIDENTIELLES			
	Code Pénal art L 226-13 Pour les fonctionnaires : loi du 13-07-83 art. 26, mais l'art. 40 du Code de Proc. Pénale fait obligation de dénoncer les crimes et délits	1 an , 100 K.F. Sanctions statutaires en sus du pénal	Théoriquement, amende jusque 500 K.F. Dommages et intérêts (cf. ci-dessus). Idem
PROTEGER LE SECRET DES CORRESPONDANCES			
	Code Pénal art. 226-15 al. 2	1 an , 300 K.F.	Théoriquement jusque 1,5 M.F.
PROTEGER L'ORDRE PUBLIC			
- protection des mineurs	Code Pénal - art 227-23	5 ans, 500 K.F.	Responsabilité pénale de l'employeur engagée Fourniture de moyens ; en principe, 5 fois l'amende prévue pour les personnes physiques.
- protection de la dignité humaine	- art 227-24	3 ans, 500 K.F.	

5.3.Protéger les systèmes informatiques

Obligation	*Fondement légal*	*Sanctions en cas de manquement*	
		personnes physiques	*personnes morales*
PROTEGER LES SYSTEMES INFORMATIQUES			
	Code Pénal (repris de la loi " Godfrain ")		Responsabilité des personnes morales :
- ne pas accéder ou se maintenir frauduleusement	- art 323-1	1 an, 100 K.F.	art. 323-6 du Code Pénal
- ne pas altérer les données ou le système	- art 323-1 al. 2	1 ans, 200 K.F.	5 fois l'amende prévue pour les personnes physiques
- ne pas entraver ou fausser leur fonctionnement	- art. 323-2	3 ans, 300 K.F.	Peines complémentaires prévues par les art. 131-38 et 131-39 (cf. ci-dessus)
- ne pas modifier frauduleusement les données	- art. 323-3	3 ans, 300 K.F.	
	- art 323-5	Peines complémentaires : - interdiction de droits civiques, civils, d'exercice de l'activité, publication du jugement par tous moyens de presse, etc.	

5.4. Obligation de l'employeur

Obligation	*Fondement légal*	*Sanctions en cas de manquement*	
		personnes physiques	*personnes morales*
Proportionner le contrôle au but recherché	Code du Travail - L 120-2		- Nullité des procédures. - Dommages et intérêts (contentieux prud'homal). - Intervention possible de l'Inspection du travail.
Informer le salarié	Code du Travail - art L 121-8		- Nullité des procédures. - Dommages et intérêts (contentieux prud'homal).
Informer préalablement les organismes paritaires concernés	Code du Travail (pour le secteur privé) - L 432-1 (consultation) - L 483-1 (délit d'entrave)	Cadres dirigeants 1 an, 25 K.F.	Délit d'entrave : - 5 fois l'amende prévue pour les personnes physiques. - Nullité des procédures engagées.
	Décrets spécifiques pour les Administrations sur le fonctionnement des C.T.P.		- Nullité des procédures engagées.

5.5. Transparence au niveau des instances représentatives

Obligation	*Fondement légal*	*Sanctions en cas de manquement*	
		personnes physiques	*personnes morales*
Information préalable des organismes paritaires concernés	Code du Travail (pour le secteur privé): - art. 432-2-1 (consultation) - art. 483-1 (délit d'entrave)	Cadres dirigeants 1 an, 25 K.F.	Délit d'entrave : - 5 fois l'amende prévue pour les personnes physiques - nullité des procédures engagées
	Décrets spécifiques pour les Administrations sur le fonctionnement des C.T.P.		- Nullité des procédures engagées

5.6. Loi sur la Sécurité Quotidienne : adoption de la loi le 31 octobre 2001

D'un contenu sécuritaire très dense et couvrant de multiples domaines, la LSQ a des conséquences très importantes pour les entreprises et notamment pour les opérateurs et fournisseurs télécoms et les établissements financiers.

Sans entrer dans les différents compartiments de cette loi, quelques points doivent être pris en compte dans l'élaboration de la charte d'utilisation :

- La durée de conservation des logs ;
- Les éléments de logging qui permettront de déterminer des profils divers : goûts et centres d'intérêts ;

- La notion de « terrorisme », de périmètre assez flou, commence à entrer dans le domaine économique : la nécessité d'une classification des informations en entreprise est un préalable à l'encadrement de l'usage de la messagerie ;
- La lutte contre le blanchiment d'argent et le support indirect au terrorisme implique pour les entreprises concernées directement - le secteur financier -, ou indirectement - secteur high tech -, un renforcement des moyens d'audit et de sécurité : traçabilité des fonds, suivi des informations sensibles ;
- Le droit d'auteur semble aussi être quelque peu bousculé : c'est l'auteur dont la publication est attaquée qui devra prouver le caractère licite de celle-ci.

Nous invitons le lecteur à relire sous l'angle de la sécurité des systèmes d'information les différentes prises de position publiées sur Internet
.

6. Les risques et conséquences

Exemples de risques	Contexte ou commentaires	Impact possible : Pertes quantifiables	Autre pertes (non quantifiables)	Engagement de la responsabilité civile	Engagement de la responsabilité pénale	Actions préventives possibles
ATTEINTES A LA CONFIDENTIALITE						
Atteintes à la sécurité des informations nominatives (divulgation, défaut de sécurité)	Transmettre des informations nominatives en clair par **Messagerie** (media absolument non sécurisé) est déjà *en soi* une atteinte à leur sécurité !	Frais de justice, dommages-intérêts	Contre-publicité	Entreprise et salarié responsable	Du salarié responsable, et de l'entreprise pour défaut de sécurité	Sensibiliser le personnel Classifier les informations Définir les procédures et auditer Utilisation de moyens sécurisés
	Annuaire ou application de gestion diffusant abusivement des informations nominatives sur le **Web**. L'avis des personnes concernées a été ignoré alors qu'elles peuvent s'opposer à une telle diffusion		Conséquences parfois désastreuses (vie privée des collaborateurs)			
Divulgation d'autres informations sensibles	Par la **Messagerie** : action volontaire ou non : erreur, copie cachée,	Pertes d'exploitation Pertes de patrimoine informationnel (savoir-faire technique)	Atteinte à l'image de l'entreprise, à plus ou moins court terme Dysfonctionnement grave de l'entreprise	De l'entreprise, si contrevient à un contrat avec un tiers	Possible (a apprécier selon le contexte :)	Classifier les informations Sensibilisation
	Par les **Forums** Divulgation directe ou par la connaissance des abonnements, permettant de cerner les centres d'intérêt de l'entreprise **Web** : cf. les « cookies »					

Exemples de risques	Contexte ou commentaires	Impact possible :				Actions préventives possibles
		Pertes quantifiables	Autre pertes (non quantifiables)	Engagement de la responsabilité civile	Engagement de la responsabilité pénale	
Atteinte au secret de correspondance	Par les outils de contrôle de la **messagerie**	Frais de justice, dommages-intérêts	Image de l'entreprise si l'affaire devient publique	De l'entreprise et du salarié responsable	Du salarié responsable, et éventuellement de l'entreprise	Se reporter au chapitre sur la mise en œuvre de la charte
Traitement non autorisé d'informations nominatives	Par les fichiers « logs »ainsi que pour ceux relatifs au proxy (**Web)** Annuaires non déclarés sur le **Web**	Frais de justice, dommages-intérêts	Image de l'entreprise si l'affaire devient publique	De l'entreprise et du salarié responsable	Du salarié responsable, et éventuellement de l'entreprise	Se reporter au chapitre sur la mise en œuvre de la charte Déclaration à la CNIL
UTILISATIONS ILLICITES						
SPAM (envoi de messages non sollicités, gênants)	**messagerie** Pour des raisons propres à l'utilisateur (jeu, ressentiment…), ou si le serveur est mal configuré et sert de relais	Perte d'exploitation, en cas de liaison non permanente facturée à la durée. Dommages-intérêts éventuels	L'entreprise peut être « blacklistée » (figurer sur la liste des sites pratiquant le *spamming*) et ne peut plus échanger de mails	Possible	Possible si évolution de la législation en la matière (cf. Loi sur la Sécurité Quotidienne, oct. 2001)	Formation (outil, bon usage du Net…) Sensibilisation Paramétrage du système
Utilisation non professionnelle abusive (trop fréquente)	**Messagerie** et **web**	Perte d'exploitation (cf ci-dessus)	Perte de temps			Charte d'utilisation
Infections informatiques *(Certains virus rendent possible les intrusions, et donc la **divulgation d'informations** (cf. ci-dessus))*	En **messagerie**, par les fichiers attachés au message ou plus rarement le message lui-même (cf : virus « KAKWORM ») Téléchargement par le **web** de logiciels douteux Le contrôle anti-virus du webmail dépend souvent de la station cliente	Frais de reconstitution d'information, de décontamination, et frais annexes (expertise extérieure..) Dommages-intérêts si vous infectez vos correspondants		Possible pour l'entreprise, si vous transmettez l'infection à une autre entreprise	Seulement si l'élément intentionnel est prouvé (rare, mais…)	Procédures Sensibilisation Antivirus au niveau de la messagerie et des postes, mis à jour fréquemment Veille

Exemples de risques	Contexte ou commentaires	Impact possible :				Actions préventives possibles
		Pertes quantifiables	Autre pertes (non quantifiables)	Engagement de la responsabilité civile	Engagement de la responsabilité pénale	
Usurpation d'un authentifiant	« Emprunter » l'identifiant et le mot de passe d'un collègue : au niveau de la **messagerie**, ou serveur **web** auquel l'entreprise est abonnée	Pertes financières (selon la nature du serveur web) Dommages-intérêts si un litige s'ensuit	Forte atteinte possible à l'image de l'entreprise Dysfonctionnnements dans l'entreprise Perte de traçabilité des actions	Possible pour l'entreprise, si usurpation de l'identité d'un responsable	Celle de l'usurpateur, le cas échéant	Charte et sensibilisation
Déni de service (bande passante est saturée : ressources réseau indisponibles…)	**Messagerie** :messages trop nombreux et/ou volumineux **Web** : téléchargements volumineux et répétés « Jouer au pirate » en utilisant une URL adéquate	Coûts de connexion (éventuellement) Pertes commerciales (commandes bloquées) Dommages-intérêts	Image de l'entreprise, selon les cas	Possible si un contrat lie l'entreprise, avec des délais d'intervention à respecter par exemple	Le cas échéant, celle du fautif	Idem + paramétrage des systèmes
EXPRESSIONS NON AUTORISEES						
Prise de position non autorisée engageant l'entreprise	Au niveau de la **messagerie** et des **forums.** Usurpation de fonctions, en quelque sorte…	Dommages-intérêts si un litige s'ensuit	Forte atteinte possible à l'image de l'entreprise, à son fonctionnement et à son ambiance de travail	Possible pour l'entreprise	A voir selon les cas	Organiser la politique de communication extérieure de l'entreprise Etablir une Charte d'utilisation
(Re) diffusion de fausses nouvelles (messages « hoaxes »)	Utilisation crédule ou malveillante de la **messagerie**	Frais de justice, Dommages-intérêts	Atteinte possible à l'image de l'entreprise	Celle de la personne concernée Mais possible également pour l'entreprise	Celle de la personne concernée Mais possible également pour l'entreprise, si l'élément intentionnel est prouvé, ou si une trop forte négligence le laisse penser…	
Diffamation, racisme, négationnisme, pédophilie, harcèlement…	**Messagerie** : dans le corps du message ou en fichier attaché **Web** : création d'un site non autorisé en utilisant les moyens de l'entreprise	Frais de justice, Dommages-intérêts	Forte atteinte possible à l'image de l'entreprise	Celle de la personne concernée Mais possible également pour l'entreprise	Celle de la personne concernée Mais possible également pour l'entreprise, si l'élément intentionnel est prouvé, ou si une trop forte négligence le laisse penser…	Organiser la politique de communication extérieure de l'entreprise Charte…

Exemples de risques	Contexte ou commentaires	Impact possible :				Actions préventives possibles
		Pertes quantifiables	Autre pertes (non quantifiables)	Engagement de la responsabilité civile	Engagement de la responsabilité pénale	
ATTEINTE A LA PROPRIETE INTELLECTUELLE						
Récupération ou diffusion de copies illicites de logiciels	**Web** : Téléchargement - **Messagerie** En fichier(s) attaché(s)	Frais de justice, coûts de régularisation (prix des logiciels non remisé…)	Atteinte à l'image de l'entreprise	idem	idem	Sensibilisation Charte Contrôles…
Récupération de bases de données ou de sites web	**Web** Téléchargement **Intranet** Utilisation abusive directe, ou insertion d'un lien vers un site extérieur	Frais de justice, Dommages-intérêts		Celle de la personne concernée Mais possible également pour l'entreprise	Celle de la personne concernée Mais possible également pour l'entreprise, si l'élément intentionnel est prouvé, ou si une trop forte négligence le laisse penser…	Sensibilisation Charte Contrôles…

7. Finalité d'une charte d’utilisation des moyens Intranet et Internet

Une charte d'entreprise a pour finalité d'expliciter et de clarifier :

- Les droits et devoirs du salarié en matière d'usage des moyens de communication ;
- Les obligations de l'employeur en matière de protection des informations manipulées dans et par l'entreprise ou l’administration ;
- Les limitations actuelles imposées par la législation.

Afin que le propos exprimé dans la charte d’utilisation soit formateur, il convient d'expliquer au salarié l’intégration profonde des moyens de communication dans le fonctionnement des systèmes d'information de l’entreprise. Ainsi, il doit être informé :

- du contrôle technique réalisé par le système d'habilitation ;
- du fonctionnement enregistré dans les fichiers « logs » qui constituent de facto des preuves numériques.

Aujourd’hui, les juges passent de la responsabilité pour faute objective à la responsabilité pour risque.

Dans le premier cas il faut prouver la faute, dans le second il faut informer de l’existence de techniques et prendre des mesures de sécurité. Si ces devoirs d’information et de sécurité ne sont pas remplis ; l’entreprise, à travers ses dirigeants et responsables de la sécurité, verra sa responsabilité engagée.

Contenu-type d’une charte d’utilisation des moyens Intranet et Internet

Dans cette troisième partie, le lecteur trouvera une formulation pour chacun des éléments clés devant être cités dans une charte d’utilisation des moyens intranet et internet.

Nous ne proposons pas de modèle-type. En effet, il est essentiel que la charte soit le reflet des valeurs propres de l’entreprise. Un modèle « prêt à l’emploi » amènerait naturellement le RSSI, pilote pour la création de la charte, à s'enfermer dans le style proposé. Ainsi, l’expression des « législateurs internes à l'entreprise » serait limitée, tant dans leur représentativité que dans leur niveau de responsabilité.

8. Situer la charte dans le fonctionnement de l'entreprise

A ce jour[3], si la charte d'entreprise n'a pas d'existence légale, elle n'en est pas moins incontournable. Cette absence de légalité ne simplifie ni son contenu, très vaste par définition, ni son application claire en cas de problème majeur.

Quel que soit le style et la tonalité donnée au document, une charte d'utilisation doit prendre en compte un nombre important d'éléments qui sont traditionnellement sous la responsabilité d'unités opérationnelles et fonctionnelles de l'entreprise.

Il s'agit de reformuler ces éléments suivant un axe différent afin de donner une cohérence dans le bon usage des moyens de communication.

Le Règlement Intérieur d'entreprise, sous la responsabilité de l'employeur, codifie principalement les limites et les sanctions en cas de manquement. Sans être en concurrence ni en contradiction, la charte donnera un cadre avec des conseils associés pour définir ce qu'est un comportement responsable et un bon fonctionnement pour tous.

Plus que les sanctions, la charte s'efforcera de décrire tous les moyens nécessaires pour contrôler et assurer la protection des personnes et de l'entreprise en fonction des risques encourus par le salarié et l'entreprise et des contraintes légales.

A noter que le vocable « moyens de contrôles » englobe les moyens en eux-mêmes mais aussi la manière dont ils seront utilisés. Cette définition devra être indiquée clairement.

Compte tenu de l'étendue des domaines couverts par la charte et de sa complémentarité avec le Règlement Intérieur, elle est souhaitable qu'elle soit validée par les instances dirigeantes de l'entreprise et approuvée par les **partenaires sociaux. Ces derniers pourront vérifier le caractère raisonnable, pondéré, loyal et proportionnel des règles de sécurité d'entreprise**.

[3] Date de parution de la version initiale du document.

9. Périmètres d'application

Dans ce chapitre, nous reprendrons les éléments évoqués précédemment en les regroupant suivant les thèmes de sécurité définis et encadrés par la législation actuelle.

9.1. La protection des personnes et du personnel

Ce thème cible les obligations légales dont bénéficie le salarié et celles qu'il doit respecter au profit d'autrui et de l'entreprise (Loi Informatique et Libertés).

Une charte d'utilisation des NTIC doit couvrir toutes les catégories juridiques des personnels employés :

- Secteur public : titulaires, contractuels (décret de 1988) ;
- emplois jeunes ;
- Secteur privé : contrats CDI, CDD, stagiaires, intérimaires, employés de sociétés de services en régie, étudiants en alternance.

Il n'est pas recommandé de modifier le contrat de travail. Par ailleurs, il faudra également se poser la question de la responsabilité civile du chef d'entreprise.

Les règles en vigueur doivent être opposables à chacun des utilisateurs. Ceux-ci doivent en être avertis, connaître les conséquences d'une utilisation non autorisée, avoir une définition de ce qui est autorisé. L'entreprise doit veiller à la légalité des preuves et à leur opposabilité en justice.

Selon la juridiction, les preuves sont différentes :

- au Pénal, tout est admissible, y compris l'aveu,
- au Civil, notamment pour les Prud'hommes, les preuves sont plus difficiles à opposer. Un conseil de Prud'hommes a pu en effet estimer que certains supports (documents, disque dur) n'étaient pas opposables au salarié au motif qu'ils n'avaient pas été placés sous scellés (cf. affaire IBM).

9.2. La protection des systèmes d'information informatisés

Basé fondamentalement sur la loi dite « Godfrain », ce thème rappellera les modalités retenues par l'entreprise afin de protéger ses systèmes pour satisfaire non seulement aux exigences légales mais aussi assurer sa sécurité, son bon fonctionnement et l'emploi de ses salariés.

Nous trouverons donc dans cette partie, une référence ou une description générale du mode d'administration des accès aux systèmes, ainsi qu'une première description des principes de secours et de continuité des activités.

9.3. La protection des logiciels

De façon simple et rapide, ce thème doit rappeler ce qu'est le Droit d'Auteur et le Code de la Propriété Intellectuelle.

Pour apporter un éclairage sur ce sujet peu entré dans les mœurs, il convient de décrire brièvement les risques directs :

- Un logiciel sans licence est une contrefaçon et/ou un « virus ».
- Utiliser un logiciel commercial sans avoir payé la licence peut conduire l'éditeur du logiciel à mettre en œuvre des moyens de type « virus » pour pister les contrevenants[4] (cf. les actions de la BSA).
- Détourner une œuvre en se l'appropriant est un délit réprimé par le Code de la Propriété Intellectuelle.

Dans une perspective pédagogique, une étude de cas telle que la suivante peut être menée : à partir de travaux réalisés par une personne ou une équipe de l'entreprise, le personnel sera mis dans la situation d'un auteur dont l'œuvre est piratée par des tiers.

9.4. La protection des données

Bien que couvertes par les mêmes dispositions légales, on maintient la distinction aujourd'hui quelque peu artificielle entre protection des logiciels et « protection des données » pour conserver la clarté et le bénéfice d'une démarche didactique.

Néanmoins, il sera opportun de rappeler ce que recouvre l'expression « le monde de l'information » :

1. L'information est devenue la première valeur économique.
2. L'interconnexion des réseaux, notamment l'Internet, et la diffusion massive des micro-ordinateurs ont fait exploser la production de biens et d'œuvres sous format numérique.
3. Le législateur a pris et continue de prendre en compte ces évolutions du monde numérique qui concerne toute l'activité humaine : privée, économique ou politique. Les événements du 11 septembre 2001 qui ont touché les USA ont eu des répercutions législatives dans un grand nombre d'Etats, dont la France avec les lois du 31 octobre 2001 sur la sécurité. Le Code Pénal, en suite logique, s'enrichit aussi.

9.5. La protection des informations confidentielles

Comme la plupart des autres thèmes, l'obligation de confidentialité est tout à la fois une contrainte appliquée au salarié et un droit fondamental qui lui est dû.

Les systèmes informatisés contiennent des informations très détaillées sur les clients physiques et tout manquement à la confidentialité, y compris involontaire, cible potentiellement le client, l'entreprise, les tiers (concurrence, presse, fisc, etc.). La responsabilité du salarié peut donc être très sérieusement mise en cause.

[4] Une des utilisations du " spyware " (espiogiciels).

9.6. Le secret des correspondances

La diffusion massive des messageries électroniques oblige le législateur à évoluer. Il n'en demeure pas moins que le cadre législatif actuel est clair et que les pénalités ne sont pas neutres :

- Fait commis de « mauvaise foi », au sens juridique de l'expression : ouvrir, supprimer ou même retarder des correspondances privées ou non, en prendre connaissance frauduleusement est passible, en Droit Pénal, de 1 an de prison et 45.734 € (300.000 F) d'amende.

9.7. La protection de l'ordre public et la sécurité des personnes

On peut utilement regrouper ces deux thèmes en se référant aux conséquences qui potentiellement impactent l'intégrité de la personne : stress, dépression nerveuse, maladie et en cas extrême, suicide.

Ce thème cible tout ce qui porte préjudice à la dignité humaine : propos violents, diffamatoires, diffusion et accès à des informations pédophiles.

Au-delà de ces sujets, il convient de rappeler le potentiel et le danger des moyens de communication électroniques. Mêmes effacées, les informations licites et illicites demeurent sur les machines qui ont participé à la navigation. Les traces de navigation sont enregistrées.

10. Modalités d'application

10.1. Les règles de preuve

10.1.1. Le contrôle de la messagerie électronique

a) Contrôle de l'usage : Consultation du comité d'entreprise, ou du comité technique paritaire pour le secteur public.

- Article L432-2-1 Code du Travail (articles équivalents pour la fonction publique).
- Article L432-2-2 Code du Travail (conditions de travail).
- Traitements automatisés de la gestion du personnel.

Il s'agit d'une obligation de consultation du CE et non d'une nécessité d'autorisation.

b) Contrôle du contenu : Secret de la correspondance.

- Article 226-15 al. 2 du Code Pénal (protection du secret de la correspondance).

Il est interdit à l'employeur d'ouvrir le courrier personnel de ses salariés, courrier avec mention « personnel et confidentiel ».

Cas de jurisprudence :

- La messagerie électronique est assimilée au courrier papier.
- Concernant les messages électroniques des délégués syndicaux et représentants du personnel, se reporter à la Réponse Ministérielle « Chaussy », 1er fév. 1999.
- En matière de téléphonie, délimitation de l'usage privé et de l'usage professionnel.

Par ailleurs, la CNIL n'autorise pas, sauf exception :

- L'enregistrement des conversations téléphoniques ;
- La communication des quatre derniers chiffres des numéros de téléphone (cf. Délibération n° 94-113 du 20 décembre 1994).

A noter également l'existence de décisions sur l'enregistrement vidéo des salariés.

Problématique de l'e-mail

A l'instar du courrier papier, l'e-mail est composé d'une enveloppe et d'un contenu.

Par analogie, l'enveloppe comporte des informations publiques. Cependant, l'exploitation avancée de ces informations peut se révéler préjudiciable à tout ou partie des personnes physiques ou morales, par déduction des informations notées dans les champs « destinataires », « copies », « copies cachées » et « objet du message ».

Si le corps du message, privé par nature, peut seul lever toute ambiguïté d'interprétation, le traitement décrit ci-dessus peut autant constituer un faisceau de preuves stables qu'un ciblage d'intelligence économique.

10.1.2. Le contrôle des connexions sur les sites web

C'est une technique de filtrage / listage des sites mise en place par l'employeur. C'est donc un traitement automatisé de données nominatives.

Les techniques de filtrage téléphonique (interdiction du 3615, de certains 080x) ne nécessitent pas aujourd'hui une consultation du CE. On ne parle ici que du filtrage, pas de l'opposabilité de la preuve en question.

Les enregistrements et traitements nominatifs permettant l'établissement de la preuve doivent être déclarés à la CNIL.

Concernant l'intranet : la charte doit expliciter ce que les responsables de publication peuvent faire et ne pas faire (cf : § 5.6 de ce document : respect du droit d'auteur). Le cas des hyperliens est très discuté car ils sont assimilés à une représentation de l'œuvre.

10.1.3. Autres points à examiner

L'usage des forums sur Internet et le téléchargement de logiciels sont à adapter aux risques économiques de l'entreprise.

Classiquement, la participation active à un forum représente trop de risques pour l'entreprise pour que ce média soit banalisé. A défaut d'interdiction simple, un encadrement procédural est incontournable.

Le téléchargement des logiciels est plus simple à traiter. Pour éviter les risques de « piratage » de logiciels, le plus simple est d'encadrer cette fonctionnalité dans la définition de poste des personnes qui ont en charge la maintenance du parc informatique, la mise à jour des logiciels, etc.

10.2. Mesures générales mises en œuvre

10.2.1. Organisation de la sécurité d'entreprise

L'organisation de la sécurité d'entreprise par défaut est claire : le dirigeant d'entreprise, ainsi que les acteurs liés à la responsabilité hiérarchique ou opérationnelle de la sécurité informatique, sont pleinement responsables devant la Loi.

Une organisation explicite peut modifier significativement les champs de responsabilités, notamment via la définition de fonctions telles que Responsable de l'Audit Interne, Directeur de la Sécurité, RSSI, Directeur des Systèmes d'Information, etc.

10.2.2. Classification des contenus

Peu de chartes aujourd'hui indiquent quelles sont les informations que les salariés ont le droit de faire sortir de l'entreprise.

D'où un problème de classification des données loin d'être neutre pour les entreprises privées ne travaillant pas avec des organismes d'état (armées, par exemple).

10.2.3. Administration des accès

Basée sur le document publié de « Politique générale de sécurité d'entreprise », la gestion des accès aux ressources informatiques doit faire l'objet d'une administration formalisée.

10.2.4. Règles concernant les fichiers de journalisation

Comme évoqué précédemment, les fichiers « logs » constitue de facto une surveillance très détaillée de l'activité des salariés.

L'utilisation des informations contenues dans ces fichiers « logs » doit être rigoureusement encadrée afin que l'entreprise, et notamment ses responsables sécurité, ne voient pas leur responsabilité pénale engagée (cf. annexes sur la jurisprudence française 2001).

Une approche consiste à présenter dans la charte la spécificité des salariés dits " sensibles " (RSSI, administrateurs de la sécurité des postes de travail, administrateurs de la sécurité des réseaux) et d'en annexer une synthèse sur leur champ d'intervention et les modalités légales associées.

11. Eléments de contenu d'une charte

11.1. Généralités

11.1.1. Remarques préalables

Les éléments indiqués ici ne prétendent pas constituer une « charte-type », ce qui serait totalement impensable compte tenu de la diversité des cultures d'entreprise et de la législation actuelle.

L'objectif est de fournir au R.S.S.I. les données utiles, soit pour enrichir une charte d'utilisation existante, soit pour construire un document spécifique. Il est essentiel que ce document s'accompagne d'une démarche active de sensibilisation auprès des utilisateurs.

11.1.2. Le contexte des nouvelles technologies

La mise à disposition de moyens Internet ou Intranet résulte d'une volonté de l'entreprise de faciliter l'accès à l'information pour ses différents collaborateurs, sous tendue par des considérations qui lui sont propres (commerciales, image de marque,…).

Toutefois, peu de décideurs et encore moins d'utilisateurs sont conscients que l'usage relativement aisé de ces outils performants peut s'avérer potentiellement à très haut risque pour l'entreprise et pour eux-mêmes.

Il faut donc provoquer une prise de conscience globale de l'entreprise en tant que communauté. Face aux risques évoqués et à des facteurs de risque sans cesse renouvelés, la participation active, la capacité de réaction et l'adhésion de chaque acteur doivent être recherchées.

La mise en place ex abrupto d'un contrôle quasi-policier, matérialisé par une liste de prohibitions énoncées sans justification, peut faire obstacle à la créativité et à la productivité des salariés.

11.1.3. Objet de la charte

La charte doit être présentée comme un ensemble de bonnes pratiques d'utilisation des outils Internet ou Intranet s'imposant à tous les utilisateurs, et non comme une collection d'interdits. Il peut cependant exister des cas particuliers où l'entreprise, soumise à des contraintes juridiques fortes, adoptera un ton plus réglementaire qui traduira sa culture propre.

Le préambule définira **l'objet de la charte** comme recueil des règles de déontologie, de sécurité et de respect de la loi, ainsi que **le public visé** ; des personnels de statuts très différents nécessiteront peut-être plusieurs documents.

Si dans l'entreprise existent des documents formalisant la politique générale de sécurité des systèmes d'information, le préambule y fera clairement référence. Il indiquera les règles qui s'imposent à chacun dans l'intérêt de la communauté : les transgresser peut conduire à engager sa responsabilité civile ou pénale, ainsi que celle de l'entreprise, et s'exposer à des sanctions diverses.

Les règles peuvent évoluer en fonction de la technique, et/ou des caractéristiques de la délinquance informatique.

Il peut être utile de bien définir *a priori* le sens de certains termes utilisés dans la charte.

11.1.4. Les acteurs et leurs responsabilités

En fonction des caractéristiques et de la culture de l'entreprise, il est souhaitable de rappeler très précisément les responsabilités des différents acteurs, en particulier :

- qui est habilité à demander des mesures de surveillance ;
- qui gère ces moyens de surveillance et manipule les informations ainsi recueillies ;
- qui contrôle et vérifie la conformité des mesures de sécurité.

Il est généralement attendu de l'utilisateur final une utilisation rationnelle et loyale. Il peut aussi être incité à une attitude plus réactive : par exemple, faire remonter les incidents ou phénomènes anormaux qu'il constate auprès du service informatique ou du help-desk qui auront reçu des consignes particulières.

Dans une perspective d'implication forte de l'utilisateur final, nous suggérons qu'il puisse être force de proposition pour faire évoluer la charte, selon des modalités propres à l'entreprise.

11.2. Outils Internet / Intranet

11.2.1. Messageries

Cette appellation recouvre en fait trois outils :

- la messagerie interne ;
- la messagerie externe ;
- le « webmail » qui est, vu de l'utilisateur, un habillage « web » de la messagerie externe.

Il faut bien insister sur le fait que ceux-ci présentent pour l'essentiel les mêmes problématiques sécuritaires :

- l'adresse d'émission peut être usurpée ;
- le message peut être adressé en copie cachée à certains destinataires ;
- le contenu peut avoir été intercepté et/ou altéré ;
- les fichiers attachés sont des vecteurs d'infections ;
- le message d'origine peut être réexpédié par le destinataire, à un ou plusieurs correspondants ou à une liste de diffusion ;
- des messages trop volumineux et/ou trop fréquents saturent la liaison.

Ce média n'est absolument pas sécurisé, et l'utilisateur devra en tenir compte s'il veut transférer des informations, qu'elles soient confidentielles ou non.

De la même façon qu'avec un autre média, s'exprimer de façon irréfléchie ou malveillante par ce canal peut conduire à des situations conflictuelles.

11.2.2. Sites Web

Il s'agit ici de la consultation de pages HTML, de téléchargement de fichiers comprenant éventuellement des images ou du son digitalisés.

L'utilisateur doit être conscient que :

- une page web n'a rien de commun avec un document texte : données et traitements (codes exécutables normaux et/ou malveillants) y coexistent sans que cela apparaisse ;
- le téléchargement de logiciels douteux peut amener une infection informatique et dans le pire des cas une attaque économique contre l'entreprise ou ses personnels ;
- la navigation qu'il effectue peut générer à son insu une surcharge de trafic et pénaliser voire bloquer le réseau d'entreprise ;
- les cookies permettent de tracer ses consultations et de connaître ses centres d'intérêts et ceux de l'entreprise.

Si l'entreprise est abonnée à des serveurs web payants ayant un caractère transactionnel, au sens informatique du terme, une gestion non rigoureuse des mots de passe peut amener des utilisateurs non habilités à avoir accès aux informations, y compris en modification de données.

La diffusion de données nominatives par le web (exemple : annuaire) peut exposer à de lourdes sanctions si la loi n'est pas respectée.

Certains services disponibles sur le Web tels que le "webmail", qui consiste à offrir à l'internaute une boîte à lettres accessible en protocole HTTP, présentent des risques particuliers. Ils devront faire l'objet d'une analyse complémentaire en terme de lutte anti-virale mais aussi en terme de confidentialité des correspondances, certains fichiers temporaires mémorisant des informations au-delà de la session.

De plus, le partage de poste entre plusieurs utilisateurs, le partage d'espaces disque, le nomadisme et la réplication de base posent le problème de la persistance ou de la duplication d'informations personnelles bien au-delà de la fin d'une session de travail.

Ce contexte devra faire l'objet d'une étude détaillée car il permet l'accès, illégal à ce jour, aux données personnelles d'un utilisateur par un autre utilisateur (qui peut être un administrateur de sécurité du poste de travail, un support technique, etc.) et aux traces laissées par les utilisateurs précédents.

Ce contexte présente un risque très important en terme de confidentialité et d'intégrité.

11.2.3. Forums

Les risques majeurs sont principalement de deux sortes :

- porter atteinte à l'image de l'entreprise par des propos tendancieux ou simplement non autorisés ;
- faire connaître les centres d'intérêt de l'entreprise. On se situe là dans une problématique d'intelligence économique ciblant l'entreprise et/ou certains de

ses intervenants, au moyen d'un abonnement réalisé à partir d'une messagerie professionnelle.

11.2.4. Intranet

Par intranet, on entend le « web privé de l'entreprise « . Les technologies utilisées étant globalement les mêmes, les risques sont similaires.

L'utilisation d'applications multimédia extérieures à l'entreprise, ou la création de liens vers ces mêmes applications peut entraîner des problèmes de droit d'auteur.

11.2.5. Extranet

Il s'agit d'un intranet auquel ont accès des utilisateurs extérieurs aux locaux de l'entreprise.

Outre ceux déjà signalés pour le Web et l'Intranet, les risques sont par ailleurs ceux de la gestion des accès au réseau de l'entreprise depuis un réseau public.

Compte tenu de sa complexité, ce point nécessite des développements qui sortent du cadre de ce document.

11.3. Recommandations générales

11.3.1. Protection des informations confidentielles, nominatives ou non

Si une classification des informations a été définie au sein de l'entreprise, la charte doit y faire naturellement référence.

L'utilisateur est invité à respecter la confidentialité et l'intégrité des informations, à ne pas consulter celles pour lesquelles il n'est pas habilité. (Par exemple, sur le web, les bases de données ou les informations à caractère personnel comme la boîte à lettres d'un autre utilisateur). On fera le cas échéant référence au document définissant les modalités d'habilitation.

S'agissant de la sécurité des informations nominatives, on attire l'attention des utilisateurs sur **l'obligation de résultats** qu'exige la loi de 1978 ou le Code Pénal. En soulignant que la CNIL autorise un traitement et non simplement la détention de données, on veillera à ne pas en détourner la finalité, ce qui est un délit. La mise à disposition *via* le web d'informations nominatives issues d'applicatifs internes nécessite une nouvelle demande d'autorisation auprès de cette Commission.

Chaque personne concernée est en droit de refuser une telle diffusion d'informations et peut changer d'avis si elle avait accepté dans un premier temps.

Il est suggéré de déconseiller, voire d'interdire, le transfert d'informations nominatives par l'intermédiaire d'une messagerie « standard ». Les grandes entreprises ont en principe recours à des moyens d'E.D.I. sécurisés et plus adaptés. A défaut, les utilisateurs devront utiliser des moyens de chiffrement et de scellement autorisés et encadrés.

En fonction du niveau de sensibilité économique du secteur d'activité de l'entreprise, l'inscription à des forums se fera sans utiliser le compte de messagerie à usage professionnel.

Dans le même esprit, les utilisateurs pourront être invités à effacer les cookies sur leur disque dur résultants de leurs navigations sur le web.

11.3.2. Etre un utilisateur responsable

Dans le cadre d'un usage loyal et responsable, l'utilisateur se doit de respecter les autres acteurs et de ne pas transgresser la loi. Attentif aux ressources auxquelles il a accès, qui sont la propriété de l'entreprise, il a la charge de la sécurité à son niveau et applique les consignes de sécurité définies par les instances d'entreprise.

Il lui sera précisé en particulier que les droits d'accès sont personnels, et qu'ils disparaissent avec le départ du collaborateur de l'entreprise. Ils ne peuvent être en aucun cas transmis à des tiers sans autorisation. Il est nécessaire de rappeler ici les conseils liés à la protection du mot de passe. De même, il ne saurait être question d'utiliser un autre compte que le sien, sauf cas de force majeure dûment et autorisé au préalable.

Il sera incité à s'abstenir de modifier les paramétrages des systèmes, en lieu et place des personnes autorisées, d'adjoindre ou d'utiliser des dispositifs logiciels ou matériels ayant pour conséquence de perturber les systèmes, en particulier de sécurité, ou de les contourner (modems, webmail, etc.). Les anomalies de fonctionnement et les problèmes inexpliqués seront signalés au service adéquat.

Les règles d'utilisation de la messagerie et du web, telles que la taille maximale des messages, l'interdiction de « spamming », seront décrites. L'utilisation personnelle raisonnable pourra être autorisée, tant qu'elle n'affecte pas de manière significative les performances ou la sécurité des systèmes, et qu'elle ne tombe pas sous le coup de la loi. Les caractéristiques des messages à caractère privé seront précisées.

L'utilisateur peut également être dissuadé de télécharger depuis Internet des exécutables à l'origine non contrôlée par les experts de l'entreprise et de les installer sur les systèmes, et à plus forte raison de se livrer, par simple curiosité, à différentes « expériences » à base de virus ou de failles de sécurité.

11.3.3. Ne pas mettre en difficulté l'entreprise

L'utilisateur devra se garder de toute expression pouvant être pénalement sanctionnée ou de prise de position non habilitée engageant l'entreprise. Il ne doit pas se faire le relais de rumeurs ou d'informations mal fondées.
En cas de doute, une démarche doit lui être indiquée aux fins de vérification et de conduite à tenir.
Ce genre de problème peut se rencontrer à l'occasion de la création de contre-sites de salariés qui apparaissent parfois lors de certains conflits en entreprise.

11.3.4. Respect de la propriété intellectuelle

On veillera à ce que le téléchargement de tout objet (images, textes, logiciels, etc.) et la mise à disposition d'applications multimédia respectent le Code de la Propriété Intellectuelle, par le paiement des redevances logicielles et des droits d'auteur.

11.4. Modalités de contrôle de l'utilisation

La transparence au niveau du contrôle doit être la règle. Il faut mentionner l'existence de moyens de filtrage/interception a priori ou de contrôle a posteriori, et informer les utilisateurs sur les modalités de contrôle et les critères appliqués :

- raisons de sécurité ;
- nom du responsable habilité à demander un contrôle ;
- types d'informations stockées, moyens et durée du stockage ;
- délimitation des personnes ayant accès à ces informations ;
- délimitation de l'usage de ces informations.

Dans le dernier cas il sera fait référence aux fiches de fonction qui doivent encadrer les activités des administrateurs réseau ou système.

Les modalités d'information des représentants du personnel seront précisées.

Dans tous les cas, la déclaration du système de contrôle auprès de la CNIL est impérative.

Il est envisageable d'intégrer les résultats dans le bilan social. Les CHSCT (Comités Hygiène Sécurité et Conditions de Travail) ou tout autre organisme paritaire habilité peuvent aussi être associés au suivi des incidences de la surveillance électronique.

11.5. Prise de connaissance de la charte par l'utilisateur

Dans l'hypothèse de sa signature par l'utilisateur, la charte ne saurait réellement avoir le caractère d'un engagement formel et librement consenti.

La modification du contrat de travail n'est pas recommandée.

Il nous semble plus raisonnable de proposer la signature d'un accusé de réception du document et de lier par références croisées le Règlement Intérieur et tous les documents de sécurité des systèmes d'information de l'entreprise.

12. Comment élaborer une charte

12.1. L'équipe Projet

Dès lors qu'il a été démontré qu'une charte de sécurité d'entreprise recouvre les domaines juridiques, métiers (savoir et savoir-faire) et informatiques, la rédaction du document doit être un projet collectif.

Suivant la culture de l'entreprise, son mode de fonctionnement et les valeurs qu'elle affiche, le groupe Projet sera confié soit à un nombre limité de personnes expertes dans leur domaine respectif, soit à un panel représentatif des différentes directions de l'entreprise.

Quel que soit le mode projet retenu, un système de validation (exactitude et légalité du contenu de la charte) et d'approbation (direction de l'entreprise) sera mis en place pour que la charte devienne un document d'entreprise fiable, exploitable et reconnu par tout le personnel.

La composition minimale du groupe projet comprendra les fonctions-clés : les ressources humaines, le juridique, la communication, le marketing, la fonction « cœur de métier de l'entreprise » et l'informatique (réseaux et systèmes).

Il apparaît normal de confier le pilotage opérationnel de ce groupe projet au responsable de la sécurité de l'information ou à son équivalent.

Il convient de souligner que l'information préalable des partenaires sociaux et même leur participation ne peut qu'augmenter la reconnaissance de la charte comme document de référence de l'entreprise. Ainsi, l'impact sur le fonctionnement des différentes unités de l'entreprise pourra être positif.

12.2. Les références

Il est conseillé que le RSSI se renseigne sur la position retenue par les autres entreprises du même domaine d'activité économique.

Constatant une évolution rapide de la législation française, nous invitons le RSSI à vérifier la conformité de chaque point « *il est interdit de … »* et d'évaluer les conséquences possibles de toute automatisation ou de facilité accordée au salarié.

Dans une entreprise multinationale, chaque législation et leur niveau d'inter-cohérence devront être évalués avec soin.

13. Assurer le succès d'une charte

13.1. Le marketing

Comme tout produit ou service offert, la charte d'entreprise devra faire l'objet d'une réflexion marketing pour que son adoption et son appropriation par la Direction et le personnel soient un succès.

Aujourd'hui, si des règles précises existent pour l'affichage et la diffusion de documents (Règlement Intérieur, tracts syndicaux), il n'en va pas de même pour une charte concernant la sécurité liée au NTIC.

Il est donc possible à ce jour de choisir un média et des modalités plus adaptés et plus efficaces que ces modèles.

Un support original pour ce type de document suscitera l'attention et l'envie de le consulter. Une attention particulière sera portée à la présentation et à l'illustration, comme : des dessins humoristiques, de l'interactivité « auto-sensibilisation/auto-éducation », des cas types en fonction des utilisateurs.

Les supports seront par exemple :

- L'intranet de l'entreprise ;
- Une version CD personnalisée par type d'utilisateur (métier et responsabilité) ;
- Une version papier ;
- Des guides en ligne (help) appelés par l'applicatif lors de l'accès initial (messagerie, accueil des SI, etc.) et qui rappellent opportunément la section concernée de la charte.

14. Déployer une charte

14.1. Charte de sécurité et Règlement Intérieur

N'étant pas à ce jour un document légal, la charte de sécurité d'entreprise ne peut ni ne doit se substituer au Règlement Intérieur de l'entreprise.

Une approche de plus en plus retenue consiste à citer dans celui-ci son existence et son applicabilité, sans en reprendre le contenu, même synthétisé. En effet, en cas d'évolution du contenu, le Règlement Intérieur doit être à nouveau soumis pour avis au CHSCT, puis au comité d'entreprise ou d'établissement et être communiqué à l'inspection du travail.

14.2. Charte et contrat de travail

Modifier un contrat de travail valide n'est pas une opération banale et peut conduire à des départs non souhaitables en cas de refus de signature de l'avenant. Il est donc fortement recommandé de ne pas procéder de cette façon.

Lors de nouveaux recrutements, la charte doit être utilisée pour éventuellement préciser ou référencer certains points spécifiques dans le contrat de travail.

Cette approche permet une réelle souplesse tant dans le fonctionnement que dans les aspects légaux dont l'évolution est contrainte par l'usage massif des NTIC.

14.3. Charte et description de fonction

La fiche « Description de Fonction » permet à l'entreprise et au manager d'expliquer précisément les exigences de sécurité liées à la fonction.

Ce document permet d'affiner, pour un administrateur sécurité réseau, le champ de ses responsabilités et les limites des opérations de contrôles qu'il doit et peut techniquement conduire dans l'expression de son métier.

Classiquement, les obligations de confidentialité, les types de relations avec les autres unités et les reportings associés peuvent être très détaillés dans la fiche de fonction.

14.4 Comment contacter chaque intervenant ?

Le déploiement initial de la charte doit être abordé comme un projet d'entreprise.

Une communication hiérarchisée est une approche classique qui peut être utilement retenue pour faire passer le message avec l'appui de la Direction Générale.

Une communication concertée et pilotée par le manager d'unité et le RSSI permet tout à la fois d'asseoir le rôle prépondérant et la responsabilité du manager en matière de sécurité et d'affirmer la mission de conseil et d'aide que doit fournir le RSSI à tous les intervenants.

Lors de l'arrivée d'un nouvel intervenant, qu'il s'agisse d'un collaborateur ou d'un prestataire de services, les modalités seront par nature allégées et très opérationnelles.

L'entreprise communiquera au nouvel arrivant les règles de sécurité et de fonctionnement en vigueur, en même temps que ses codes d'accès nécessaires à sa mission et les références de la charte sur l'Intranet.

Par la législation actuelle, les interrogations portant sur la signature ou non de la charte par le nouvel arrivant ne sont pas levées.

15. Comment faire vivre la charte

Suivant les mêmes principes qui ont placé le RSSI comme pilote du projet d'élaboration, il apparaît qu'il demeure l'un des intervenants de l'entreprise le mieux placé pour détecter toute évolution du contenu de la charte.

Sa mission de veille qui concerne les aspects légaux, les risques liés aux NTIC et les vulnérabilités des systèmes d'information de l'entreprise, le positionne comme observateur privilégié.

Le RSSI peut proposer une réunion annuelle aux membres du groupe projet qui ont élaboré la charte. Il est entendu que ce groupe d'origine est évolutif en fonction du turn-over de l'entreprise.

Cette réunion sera l'occasion de présenter les changements intervenus dans les domaines internes ou externes à l'entreprise :

- évolution de la jurisprudence ;
- évolution des technologies, en terme d'outils mais aussi de risques et de vulnérabilités ;
- évolution de l'organisation de l'entreprise par l'appel à la sous-traitance.

Annexes

Textes applicables et jurisprudence

(*Sources consultables sur* www.jurifrance.fr *et* www.cnil.fr *)*

Textes applicables

International

- Recueil de directives pratiques sur la protection des données personnelles des travailleurs, adopté le 7 octobre 1996 par le Bureau International du Travail.

Européen

- Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales 4 novembre 1950 (art 8).
- Convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des données à l'égard du traitement automatisé des données à caractère personnel.
- Directive européenne du 14 mai 1991 sur la protection juridique des programmes d'ordinateur.
- Directive 199/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.
- Directive européenne 95/46 CE du parlement européen et du Conseil de l'Europe du 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel et à la libre circulation de ces données.
- Directive européenne du 9 avril 2001 sur le droit d'auteur.

Français

- Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par loi (227) du 11 mars 1988, loi (1336) du 16 décembre 1992, loi (548) du 1er juillet 1994, ordonnance (267) du 28 mars 1996, loi (641) du 27 juillet 1999.
- Code de procédure pénale : dispositions relatives aux atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques (art. 226-16 à 24).
- Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.
- Loi du 3 juillet 1985 sur la protection des logiciels par le droit d'auteur et loi du 1er juillet 1992 relative au Code de la Propriété Intellectuelle (CPI).
- Loi du 5 janvier 1988 dite « GODFRAIN » relative à la fraude informatique.

- Code de procédure pénale : dispositions relatives à la fraude informatique (art 323 à 441-1).

- Loi (646) du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

- Art 226-15 (N.C.P.).

- Loi (1446) 31 décembre 1992 relative à l'emploi, au développement du travail à temps partiel et à l'assurance chômage (chapitre V art 25 à 29).

- Code du Travail (principe de proportionnalité (L120-2), information préalable du Comité d'entreprise sur la mise en œuvre de moyens de contrôle des salariés (L 121-8) obligation d'informer le salarié ou candidat à l'emploi sur dispositif informatisé le concernant (L 432-2) consultation du Comité d'entreprise pour introduction de nouvelle technologie modifiant les conditions de travail (L432-2).

- Institution de la responsabilité des personnes morales (Nouveau code pénal en vigueur 1994 : art 323-6 dans conditions prévues art 121-2).

- Loi 96-659 du 26 juillet 1996 : réglementation des télécommunications et décrets d'application sur la cryptologie.

- Loi du 13 mars 2000 relative à la signature électronique.

Jurisprudence
(Sources : www.jurifrance.fr , Juris Data sur www.juris-classeur.com)

Voici un panorama jurisprudentiel, au 31 octobre 2001, limité aux aspects relatifs à la cyber-surveillance des salariés et à l'usage des outils informatiques à des fins privées. La jurisprudence étant évolutive, ces éléments devront être actualisés.

Jurisprudence française

Il existe de nombreuses décisions relatives à la cyber-surveillance des salariés et à l'usage des outils informatiques à des fins privées. La jurisprudence qui s'esquisse porte tant sur le contentieux du fond que sur celui de la preuve et affirme les principes de loyauté et de « proportionnalité ».

Il est à noter que la jurisprudence relative aux fonctionnaires est peu abondante sur ces sujets.

- Contentieux de la preuve :

- Récusation de la preuve pour un dispositif de contrôle mis en place à l'insu du salarié (arrêt de principe chambre sociale de la Cour de Cassation 20 novembre 1991).
- Récusation de la preuve rapportée par un traitement nominatif non déclaré à la CNIL (Cour d'Appel de Paris 7 mars 1997).
- Récusation de la preuve rapportée par un traitement déclaré mais sans rapport avec la finalité (Cour d'Appel de Paris 31 mai 1995).
- Exigence de la qualité de la preuve (Cour d'Appel. Aix en Provence 4/01/1994/ -Cour d'Appel de Paris 12 mai 1999).

- Contentieux au fond :

- Correspondance écrite reçue sur le lieu de travail : domaine où la jurisprudence est la plus ancienne et après avoir été univoque en faveur de la culpabilité de l'employeur ouvrant les correspondances privées (Paris 17 juin 1936 ; 18 juillet 1973)devient plus nuancée (Cass. Crim. 16 janvier 1992).
- Utilisation à des fins privées de la ligne de téléphone ou du minitel : outre la récusation de la preuve si le traitement n'est pas déclaré, dans de nombreuses affaires l'usage « abusif » du téléphone a été jugé constitutif d'une faute grave (cass. soc. 7 novembre 1995 ; Rennes, ch. soc. 30 septembre 1999) ou constituera seulement une cause réelle et sérieuse de licenciement (Nancy, ch. sociale 12 janvier 2000 ; Paris 24 février 1999) Mais la jurisprudence annulera le licenciement fondé sur l'usage privé s'il parait disproportionné aux faits de la cause. (Cas soc. 30 mars 1999), dessinant ainsi les contours d'un usage professionnel à des fins privées.
- Utilisation à des fins personnelles de l'Internet : les décisions moins nombreuses relèvent des seuls Conseils des Prud'hommes et ne peuvent constituer une généralité. Elles paraissent néanmoins témoigner d'une rigueur particulière à l'égard de l'usage à des fins privées de la messagerie électronique ou du web par la confirmation des licenciements des salariés (Cons. Prudh Paris 1 février 2000. Montbéliard 19 septembre 2000).
- Contrôle de la messagerie (1) : le Tribunal de Grande Instance de Paris, en date du 17 novembre 2000, a donné raison à un étudiant en informatique suspecté de manipulation, contre le responsable du laboratoire amené à surveiller la messagerie. Le motif retenu a été celui de violation de correspondance effectuée par la voie des télécommunications par une personne chargée d'une mission de service public. Le tribunal a considéré que la loi du 10 juillet 1991 sur le secret des correspondances émises par la voie des télécommunications s'appliquait à « toutes les communications à distance actuellement connues, dont le réseau interne et la messagerie ». Les messages électroniques des salariés sont protégés par le secret des correspondances de manière relative seulement : la loi de 1991 ne prive pas l'employeur de placer un salarié sur écoute téléphonique s'il peut prouver sa bonne foi. D'autre part, il est trop tôt pour considérer établi que la lecture d'un mail stocké sur un serveur ou sur le disque dur serait constitutive d'une interception de communication au sens de l'art. 226-15 du code pénal. Le 17 décembre 2001, la Cour d'Appel de Paris a confirmé partiellement ce jugement. Elle a admis que les administrateurs « aient accès aux messages et à leur contenu », mais elle a sanctionné la divulgation de ces mêmes contenus, en assortissant cependant du sursis les peines prononcées en première instance.
- Contrôle de la messagerie (2) : dans un arrêt du 5 octobre 2001, la Chambre Sociale de la Cour de Cassation a donné raison à un ingénieur licencié pour faute grave pour avoir exercé une activité parallèle et fait usage à des fins personnelles du matériel de l'entreprise mis à sa disposition. Cette décision s'appuie sur la Convention européenne de sauvegarde des droits

de l'homme et des libertés fondamentales, sur le Code Civil et sur le Nouveau Code de Procédure Civil. Dans cette affaire, il est reproché à l'employeur d'avoir surveillé les mails personnels de ses salariés, constitutifs de la preuve du licenciement et que cette surveillance ne respectait pas les droits fondamentaux de la personne. Il faut néanmoins nuancer les propos car :

- Il s'agissait d'une atteinte disproportionnée à la vie privée du salarié.
- Ce dernier n'avait pas fait l'objet d'une information préalable.
- C'est surtout la loyauté de la preuve qui a été jugée.

Jurisprudence européenne
(Sources : www.droit-technologie.org , www.dataprotection.gov.uk , www.registratiekamer.nl)

Transparence, proportionnalité, discussion collective sont consacrées au plan européen et la Cour européenne des Droits de l'Homme réitère l'idée que le lieu de travail n'est pas exclusif du droit de la vie privée.

Belgique :
Pour Internet, application de la jurisprudence nuancée des juridictions françaises à l'égard d'un usage à des fins privées du minitel et du téléphone. (Tribunal du travail de Bruxelles, 2 mai 2000).

Espagne :
Pas de prise en compte de la vie privée du salarié (Tribunal Superior de Justicia Cataluna, 14 novembre 2000).

Allemagne :
CEDH (23 novembre 1992) dans le cas d'une perquisition dans le cabinet d'un avocat, la Cour se fonde sur l'art 8 relatif à la vie privée de la Convention européenne des droits de l'homme et des libertés fondamentales dans les domaines de la vie professionnelle.

Royaume-Uni du 27 mai 1997 :
CEDH (23 novembre 1992) dans un cas d'écoute téléphonique, la Cour se fonde également sur l'art 8 de la Convention européenne des droits de l'homme et des libertés fondamentales dans les domaines de la vie professionnelle.

Lois étrangères et recommandations européennes de protection des données

Du panorama européen des autorités de protection des données se dégage de fortes lignes de convergence et un grand pragmatisme.
(Sources : www.dhdirhr.coe.fr).

Le commissaire britannique à la protection des données personnelles :

Après condamnation par la Cour européenne des droits de l'homme, le Royaume Uni s'est doté d'un nouveau cadre juridique relatif à l'interception des communications et aux pouvoirs d'investigations existants (Act Regulation Investigatory Powers Act). C'est la Loi britannique du 24 octobre 2000 autorisant le contrôle des salariés par l'employeur (contrôle des mails échangés sur le lieu de travail) et contrôle des communications électroniques par le gouvernement.

Le dispositif prévoit que les salariés doivent êtres informés des contrôles. Un projet de code de conduite pour les traitements mis en œuvre dans le cadre du travail, soumis à consultation publique en octobre 2000, préconise l'établissement d'une politique claire de l'entreprise sur les modalités d'utilisation des réseaux et le respect du principe de proportionnalité qui se matérialiserait par l'établissement d'une charte.

La Commission de la protection de la vie privée belge :

Un avis d'initiative de la Commission du 3 avril 2000, relatif à la surveillance par l'employeur de l'utilisation du système informatique au travail, s'articule autour des principes de transparence et proportionnalité.

Le Commissaire néerlandais

L'autorité de contrôle a publié sur son site un rapport sur le bon usage des réseaux qui précise que la surveillance systématique de l'utilisation des NTCI est disproportionnée et indique que le salarié fait son travail selon son propre jugement. Le mode de contrôle de son supérieur doit être le moins intrusif possible.

Evolutions en cours

En France

- Projet de loi français sur la société de l'information (PSLI)
  Approuvé le 13 juin 2001 en Conseil des Ministres. Ce projet s'articule autour de cinq parties :
  - l'accès du citoyen à l'informatique
  - la liberté de communication en ligne
  - l'e-commerce
  - le développement des réseaux à haut débit
  - la sécurité dans la société de l'information

- Consultation publique de la CNIL en mars 2001 sur la cyber-surveillance des salariés en entreprise.

- Dépôt à l'Assemblée Nationale le 18 juillet 2001 d'un projet de loi de transcription de la directive européenne du 24 octobre 1995, relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation des données, modifiant la Loi Informatique et Libertés.

- Spécificités de la directive par rapport à la loi française :

  - apport des risques liés à la circulation des données,
  - primauté des principes de fond sur la forme : d'abord conditions de licité puis droits fondamentaux et enfin procédures déclaratives,
  - recentrage des missions de protection sur les contrôles a posteriori (seuls les traitements générateurs de risques vis-à-vis des droits et libertés des personnes sont soumis à régime d'autorisation préalable ; plus de distinction entre secteur public et secteur privé ; simplification des formalités administratives pour traitements usuels,

- choix de ne pas abroger la loi fondatrice et unicité de régime juridique des différentes catégories de traitement (dont ceux relevant de la souveraineté nationale),
- renforcement substantiel des pouvoirs de la CNIL, autorégulation et délivrance par la CNIL d'homologation et de label.
- Adoption le 31 octobre 2001 par l'Assemblé Nationale du projet de loi relatif à la sécurité quotidienne.

En Europe

- Protection des données dans les institutions européennes et organes communautaires, adoptée le 30 novembre 2000 et un contrôleur européen des données devrait bientôt être normalisé.

- Proclamation de la charte des droits fondamentaux de l'Union Européenne préparée par la Convention au sommet de Nice du 7 décembre 2000 (article 8, elle renforce les dispositions sur la protection des données). La protection des données est reconnue comme l'un des Droits de l'Homme fondamentaux. Non ratifiée, la Charte est néanmoins un élément de référence.

- Reconnaissance par la Commission Européenne du niveau adéquat de protection des données pour plusieurs nouveaux pays : en Hongrie, en Suisse.

- Adoption le 14 juin 2001 par la Commission d'un modèle de clauses contractuelles type qui ont pour but d'encadrer les flux de données dans tous les secteurs économiques et au niveau mondial.

Sur le Plan international

Etats Unis
(Source *: www.clusif.asso.fr)*

- Le « safe Harbour » adapte la directive européenne sur les traitements à caractère personnel et la circulation de ces données informatiques. Le système publié par le Ministère du Commerce américain et reconnu adéquat par la Commission Européenne le 26 juillet 2000 a pour objectif d'encadrer la collecte et l'exploitation des données commerciales. Il repose sur le principe de l'autorégulation tout en satisfaisant les exigences de la Commission européenne. Baptisé « Safe Harbour », cette sphère de sécurité « recense les entreprises qui ont accepté de s'y ancrer et qui s'engagent à respecter les règles très proches de celles de la directive européenne ».

- Microsoft a annoncé le 15 mai 2001 son intention d'adhérer aux principes de la « sphère de sécurité ».

- La Federal Trade Commission (FTC), instance régulatrice des échanges commerciaux américains qui envisageaient l'an dernier la création d'une loi spécifique aux protections des données personnelles des consommateurs, notamment sur Internet, change complètement d'attitude et a annoncé le 4 octobre 2001 qu'elle entendait appliquer les législations en vigueur, sans aller plus loin.

Argentine
Adoption d'une loi de protection des données le 2 novembre 2000.

Hongkong
Organisation d'une première semaine de la vie privée (mars 2001) destinée à sensibiliser le public.
Australie
(Sources *: www.privacy.gov.au)*

Le Commissaire fédéral australien à la vie privée lance trois consultations publiques d'avril à mai 2001 sur le développement des codes de conduite, sur un guide d'application des principes nationaux pour la protection des données et sur les services de santé.

Instances internationales

- La 23è Conférence Internationale des Commissaires européens à la protection des données personnelles s'est tenue à Paris du 23 au 26 septembre 2001. La 24è Conférence se tiendra à Cardiff, Pays de Galle, du 9 au 11 septembre 2002.

- Institutionnalisation de la Conférence des Commissaires européens à la protection des données personnelles lors de la conférence de Paris, où il a été décidé de mettre en place une procédure d'accréditation de ses membres et une procédure d'adoption de résolutions.