Forum des Compétences
de la Sécurité
des Systèmes d'Information

La « charte informatique » par l'exemple

Clefs pour la rédaction et la mise en place d'une charte d'utilisation des ressources informatiques et de communication électronique dans l'entreprise

Rapport du groupe de travail
« Informatique et Juridique »

Remerciements

Le Forum des Compétences de la Sécurité des Systèmes d'Information remercie ses Etablissements Membres qui ont participé à la réflexion et à la rédaction de cet ouvrage présentant

La « charte informatique » par l'exemple

Clefs pour la rédaction et la mise en place d'une charte d'utilisation des ressources informatiques et de communication électronique dans l'entreprise dans le cadre de la protection du Patrimoine Informationnel des Entreprises.

Il tient à remercier particulièrement les membres* du groupe de travail qui ont réalisé à cet ouvrage

* Voir annexe 3

Sommaire

Introduction

Le groupe de travail « Informatique et Juridique » du FORUM des COMPÉTENCES travaille depuis plus d'un an sur la mise en place des chartes d'utilisation des ressources informatiques et des moyens de communication électronique.

Les chartes font partie du dispositif de sécurité des entreprises. Leur contenu, leur rédaction et leur place dans la hiérarchie des documents de l'entreprise soulèvent de nombreuses questions. Le groupe de travail, par un échange entre spécialistes de la sécurité et juristes, a établi un document d'aide à la réflexion et à la rédaction en tenant compte de l'expérience et d'exemples mis en œuvre dans les établissements financiers membres du FORUM des COMPÉTENCES.

I. FONDEMENTS DE LA CHARTE

I.1. RAISON D'ETRE

La charte d'utilisation des systèmes d'information représente l'un des instruments de sécurisation de l'entreprise, de sensibilisation et de responsabilisation des utilisateurs.

I.2. OBJECTIFS

Elle a pour objectif de fixer les devoirs et obligations des utilisateurs et des entreprises dans l'utilisation des systèmes d'information et de communication électronique. Elle permet notamment :

- d'informer les divers utilisateurs (salariés, intervenants externes) sur les règles qui, au sein de l'entreprise, régissent l'utilisation du système d'information,
- de les responsabiliser,
- de rappeler la réglementation,
- de fixer les règles d'une surveillance de l'utilisation,
- de protéger l'entreprise en cas de non respect des règles par les utilisateurs.

Les objectifs de la charte, quels qu'ils soient, doivent être identifiés et explicités.

I.3. LE DEVOIR ET LE POUVOIR DE CONTROLE ET DE SURVEILLANCE

Dans un environnement fortement concurrentiel et médiatisé, l'information stratégique devient une richesse qui doit être protégée. C'est pourquoi l'Etat met en œuvre une politique d'intelligence économique destinée à protéger l'économie nationale. La protection du patrimoine matériel et immatériel des entreprises mais aussi des services, notamment bancaires, conditionne la pérennité de l'activité économique nationale.

Quotidiennement, les acteurs de la vie économique sont soumis à des agressions diverses et variées occasionnant la fuite d'informations importantes dont la criminalité informatique est fréquemment l'instrument. Le marché de la concurrence s'en trouve souvent faussé.

Un chapitre complet du Code pénal est notamment consacré aux atteintes aux intérêts fondamentaux de la Nation. Il peut s'agir de la livraison d'informations à une entreprise ou puissance étrangère mais également d'atteintes au secret de la défense nationale, le terme défense nationale devant être entendu dans un sens très large et notamment économique.

De plus, le monde bancaire est soumis à des principes très stricts qui reposent notamment sur l'interdiction de divulguer les informations confidentielles relatives au compte d'un client, ce secret pouvant être seulement levé dans quelques cas prévus par la loi (réquisitions judiciaires, déclaration de soupçons…).

L'article L. 511-33 du Code monétaire et financier dispose que toute personne qui, à un titre quelconque, participe à la direction, gestion ou est employé par un établissement financier est tenue au secret professionnel sauf à l'égard de la Commission bancaire, de la Banque de France, des autorités judiciaires dans le cadre d'une procédure pénale.

L'article L. 511-34 précise cependant que les informations seront transmises aux établissements du même groupe installés dans l'Union européenne ou dans l'Espace économique européen, notamment pour la lutte contre le blanchiment de capitaux et le financement du terrorisme.

De façon générale, les entreprises ont également un devoir de sécurité (et notamment de confidentialité) des données à caractère personnel qu'elles traitent (clients, personnel…) en vertu de la loi du 6 janvier 1978 dite « Informatique et Libertés ».

Enfin, les salariés mais également des tiers extérieurs à l'entreprise peuvent, en utilisant les ressources informatiques mises à leur disposition, commettre un acte interdit par la loi pénale.

Dès lors, trois types de comportements peuvent être enregistrés :

- l'utilisation des ressources informatiques comme l'objet même de l'infraction, à l'exemple des atteintes aux systèmes de traitement automatisé de données, aux données personnelles, à l'usage de la cryptologie, ou encore aux interceptions illégales de communications.

- l'utilisation des capacités des technologies numériques et notamment d'Internet comme moyen pour faciliter, préparer ou commettre une infraction comme par exemple le blanchiment d'argent, la divulgation de données informatisées ou de fichiers de nature à nuire à la défense nationale ou aux intérêts fondamentaux de la Nation, la divulgation d'informations bancaires.

- l'utilisation des technologies numériques comme support d'une infraction de contenu comme racisme, outrage ou encore pédopornographie.

I.3.1. Droits et responsabilités de l'employeur

En vertu de son pouvoir de direction, l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail, y compris l'utilisation faite du système d'information.

Cela concerne tout naturellement la détection d'éventuels comportements fautifs de salariés susceptibles de ternir l'image de l'entreprise, voire d'engager sa responsabilité pénale et civile. Il s'agit d'ailleurs plus d'un devoir que d'un droit.

En matière pénale, la responsabilité du dirigeant suppose la commission d'une infraction par le préposé qui consistera en principe dans une faute non intentionnelle, mais également l'existence d'une faute personnelle imputable au dirigeant.

Ainsi, la violation de prescriptions légales et réglementaires par le préposé impliquera *a priori* de retenir une négligence fautive de la part du dirigeant dans son devoir de contrôle et de surveillance.

Dès lors, les juridictions pénales ont une approche très rigoureuse de ce devoir. Au sens de la jurisprudence de la chambre criminelle de la Cour de cassation du 14 mars 1979, il faudra que le préposé désobéisse au dirigeant pour que ce dernier puisse s'exonérer de sa responsabilité.

En outre, l'article 121-2 du Code pénal reconnaît la responsabilité pénale de la personne morale de droit privé en qualité d'entreprise. A l'origine, les quelques infractions concernées étaient limitativement prévues au Code pénal. Cependant, la nature des infractions susceptibles d'intéresser les personnes morales a été largement étoffée dans le Code pénal mais également dans d'autres codes comme celui de la propriété intellectuelle et certains textes spéciaux. Sont par exemple visées les infractions commises contre des systèmes informatiques (art. 323-6 du Code pénal), ainsi que les atteintes liées au traitement automatisé de données à caractère personnel prévues par l'article 226-24 du Code pénal, mais également les infractions de contenu comme des pages web qui contiendraient des messages violents ou pornographiques susceptibles d'être vus par un mineur ou encore des dénonciations calomnieuses.

En matière de loi spéciale, on pourrait citer la mise à la disposition de mineurs de certains documents de l'article 39 de la loi du 17 juin 1998 sur la protection des mineurs.

Dans le domaine du droit civil, les articles 1383 et 1384 du Code civil disposent en substance que toute victime non liée par un contrat avec une personne physique ou morale peut obtenir réparation de cette dernière à raison des dommages causés de son propre fait, de sa négligence ou de son imprudence, mais aussi de ceux causés par les personnes dont elle doit répondre ou des choses qu'elle a sous sa garde. L'alinéa 5 de l'article 1384 précise que sont responsables civilement « *les commettants du dommage causé par leurs (…) préposés dans les fonctions auxquelles ils les ont employés* ».

Dès lors, l'employeur ne s'exonère de sa responsabilité que si son salarié a agi hors des fonctions pour lesquelles il est employé, sans autorisation et à des fins étrangères à ses attributions, ces conditions étant cumulatives (décision de la Cour de cassation du 19 mai 1988).

Mais celles-ci peuvent être regardées d'une manière extensive par le juge, comme en témoigne l'arrêt « Escota » de la Cour d'appel d'Aix-en-Provence du 13 mars 2006 concernant la mise en cause de la responsabilité de l'employeur (Lucent) dans le cadre d'un site Internet au contenu illicite créé par un salarié.

Dans cette affaire, et au regard de l'analyse des magistrats, le préposé a agi dans le cadre de ses fonctions puisqu'il est technicien test dans une entreprise dont l'activité est la construction d'équipements et de systèmes de télécommunication, fonctions pour lesquelles l'usage d'un ordinateur et d'Internet doit être quotidien.

De plus, une note de service autorise les salariés et donc le préposé à « *utiliser les équipements informatiques mis à leur disposition pour consulter d'autres sites que ceux présentant un intérêt en relation directe avec leur activité* ».

Enfin, selon la Cour d'appel, il n'a pas agi à des fins étrangères à ses attributions puisque la même note de service autorise les salariés à disposer d'un accès à l'Internet, y compris en dehors des heures de travail.

I.3.2. Les limites aux droits de l'employeur

Si l'employeur a le droit de contrôler et de surveiller l'activité des salariés pendant le temps de travail, pour autant l'emploi de procédés clandestins est illicite et les moyens mis en œuvres doivent respecter les formalités préalables prévues par la loi (déclaration du traitement à la CNIL, consultation des instances représentatives du personnel…).

Les rapports hiérarchiques au sein d'une entité seront d'autant mieux acceptés et compris qu'il existe un véritable climat de confiance entre les acteurs. Il ne s'agit donc pas de donner l'impression aux salariés que pèse sur eux une véritable suspicion, voire inquisition hiérarchique. L'idée est bien d'associer tous les acteurs dans une même démarche concertée et acceptée de tous.

C'est pourquoi le principe de transparence doit être largement appliqué à l'égard des collaborateurs du service (article L. 121-8 du Code du travail), de même que les mesures prises du point de vue du droit des personnes et des libertés individuelles doivent être proportionnées au but recherché (article L. 120-2 du Code du travail), et que le comité d'entreprise doit être informé et consulté du moyen mis en œuvre (article L. 432-2 du Code du travail).

II. FORMALISATION DE LA CHARTE

II.1. STATUT ET FORMALISME

L'articulation de la charte avec les autres textes applicables dans l'entreprise est importante. Dans tous les cas, elle doit s'inscrire en cohérence avec les textes externes (la réglementation applicable) et internes existants.

En France, l'environnement juridique est composé notamment des principaux éléments suivants :

Réglementation « externe »	
Directives et décisions-cadres européennes Lois et règlements	
Réglementation interne	
Règles collectives	Règlement intérieur Chartes Instructions Notes de services, etc.
Contrats	Contrats de travail Contrats tiers (stagiaires, prestataires, fournisseurs, etc.)

L'entreprise détermine la localisation de la charte dans la « constellation » de ses règles internes, qui sont notamment le règlement intérieur, la politique de sécurité et les codes de déontologie. La valeur juridique de la charte sera liée à ce choix.

II.1.1. Statut juridique de la charte

L'entreprise peut choisir, selon son organisation, d'en faire une partie du règlement intérieur ou d'en faire un document autonome. La charte pourra bénéficier de deux statuts différents :

- Elle est juridiquement intégrée au règlement intérieur de l'entreprise. Dans ce cas, la charte peut formellement faire partie intégrante du texte du règlement ou constituer une annexe à celui-ci. Cette seconde forme permet de la modifier sans nécessairement procéder à la modification du corps principal du règlement. Quelle que soit la nature du lien avec le règlement, tout ajout de règles ou modification devra faire l'objet d'un formalisme obligatoire. D'une part, le règlement intérieur devra faire l'objet d'une information et d'une consultation des instances représentatives du personnel. D'autre part, le règlement devra être soumis à l'approbation de l'inspection du travail dont dépend l'entreprise.
  Le non-respect des obligations y figurant pourra exposer l'utilisateur salarié aux sanctions disciplinaires prévues par le règlement.

- La charte n'est pas intégrée au règlement intérieur. Elle constitue un document autonome, sous forme de note, affiche, publication interne. Dans ce cas, elle a une valeur informative, pédagogique ou morale.

Le non-respect des éventuelles obligations y figurant ne pourra faire spécifiquement l'objet de sanction.

Selon la force donnée à la charte (déontologie, caractère obligatoire), l'entreprise adaptera également la forme du texte (voir ci-après II.6 « Choix du vocabulaire »).

II.1.2. Partenaires impliqués dans la rédaction

Cela dépend des choix d'organisation interne de l'entreprise, mais également souvent de sa taille. En général, participent à sa rédaction :

- les représentants en charge de la sécurité de l'information, en particulier le RSSI,
- les représentants des ressources humaines,
- les représentants des directions informatiques,
- les représentants de la direction juridique,
- …

D'autres directions peuvent être consultées sur ce document (déontologie, conformité…)

Bien que cela ne soit en rien juridiquement obligatoire pour les entreprises de droit privé, quelques-unes d'entre elles ont rédigé leur charte en associant plus ou moins directement les représentants du personnel ou les instances représentatives du personnel.

II.1.3. Effets du non-respect de la charte

Comme cela a été brièvement abordé dans le point II.1.1, si l'entreprise fait le choix de donner un statut autonome à sa charte ou de l'intégrer dans son règlement intérieur, alors le non-respect de ses dispositions par l'utilisateur aura pour effet de l'exposer aux sanctions prévues dans ledit règlement.
Selon la nature et les circonstances des actes, les mesures suivantes peuvent s'appliquer : l'avertissement écrit, le blâme, la rétrogradation impliquant un changement de poste et le licenciement pour motif disciplinaire. Ces sanctions sont citées dans l'ordre croissant de gravité.

Si le texte n'est pas associé au règlement intérieur, il aura une valeur informative et aucune sanction relative à un manquement spécifiquement indiqué par ce seul texte ne pourra être appliquée, les magistrats considérant qu'un document établissant des règles impératives générales concernant l'hygiène ou la sécurité doit, par nature, être intégré dans le règlement intérieur et respecter son formalisme, sous peine de nullité.

Toutefois, les règles générales de loyauté dans l'exécution du contrat du travail ainsi que d'autres dispositions du règlement intérieur pourront éventuellement, quant à elles, fonder une sanction concernant les mêmes faits.

Chaque formalisme présente des avantages et inconvénients et devra être adapté aux objectifs recherchés.

II.1.4. Mode de révision de la charte

De même, le mode de révision de la charte dépendra de son formalisme d'adoption. Une modification du règlement intérieur sera soumise au même formalisme que son adoption (voir II.1 ci-dessus).
Les chartes indépendantes du règlement intérieur bénéficieront naturellement d'un mode de révision allégé.

II.2. DEFINITION DES UTILISATEURS

Le rédacteur s'efforcera de définir qui sont les utilisateurs des systèmes d'information et de communication électronique, afin d'adapter la rédaction à différentes populations soumises à des environnements juridiques différents.

Les utilisateurs peuvent notamment appartenir aux groupes suivants :

- salariés de l'entreprise,
- salariés de filiales,
- administrateurs système ou sécurité,
- intérimaires,
- stagiaires,
- prestataires.

Chacun des groupes devra être identifié, ainsi que les documents qui leur sont juridiquement opposables, afin d'adapter la charte de l'entreprise aux conditions d'utilisation et aux conditions contractuelles liant l'entreprise aux utilisateurs et éviter qu'un externe puisse utiliser le système d'information de l'entreprise sans que la charte ait été portée à sa connaissance.

Exemple :

- le règlement intérieur n'est pas opposable juridiquement aux prestataires externes. Il faut donc annexer la charte au contrat de prestations, lui donnant une valeur contractuelle opposable à la société prestataire,
- le règlement intérieur d'une entreprise n'est pas applicable aux salariés d'une de ses filiales. Il faut donc que la filiale reprenne la charte en tout ou en partie dans son propre règlement intérieur afin que le document soit juridiquement opposable à ses salariés (cas de filiales d'un groupe tentant d'harmoniser les pratiques en matière d'utilisation des systèmes d'information).

Il est également important de prendre en compte le cas particulier des stagiaires dans l'entreprise (le règlement intérieur leur est opposable mais les sanctions — tel que le licenciement, la plus forte d'entre elles — ne sont pas réellement dissuasives).

II.3. DOMAINES D'APPLICATION

La rédaction du présent guide se veut volontairement large, afin de pouvoir être une source d'inspiration pour les entreprises, quels que soient les outils concernés par la charte.
Le périmètre des outils est à définir en laissant l'ouverture nécessaire aux évolutions technologiques futures :

- micro-ordinateurs personnels fixes ou portables,
- serveurs,
- téléphonie fixe ou portable,
- messagerie électronique,
- télécopieurs et photocopieurs,
- vidéoprojecteurs,
- clés USB et autres supports,
- etc.

Une même charte peut viser l'ensemble des situations. Mais il peut également être envisagé de construire différentes chartes en fonction des usages et outils associés : PC et téléphonie, fixes ou nomades, etc, chaque document devant respecter le formalisme adéquat à la valeur juridique que l'on souhaite lui donner.

Par ailleurs, il sera utile de préciser si le texte traite principalement de l'usage des outils, ou également de la sécurité (et notamment de la confidentialité) des données, ou si ce domaine est régi par d'autres règles (contrat de travail, code de déontologie, etc.)

II.4. TEXTES DE LOI APPLICABLES

Une liste indicative non exhaustive des principaux textes existants figure en annexe 1 du présent document.

II.5. APPLICATION DE LA REGLEMENTATION ADAPTEE A LA SPECIFICITE DE L'ENTREPRISE

Outre le choix de hiérarchisation de la charte dans les règles de l'entreprise, son « positionnement » par rapport à l'interprétation de la réglementation doit être bien réfléchi car il est très structurant. Il est important de trouver un bon équilibre entre les règles applicables et la liberté des salariés.

Le rédacteur de la charte est libre de doser l'approche, plus ou moins rigoriste, qu'il aura de l'interprétation des textes en vigueur et de la jurisprudence actuelle. C'est-à-dire que la rédaction pourra être plus ou moins souple quant à un principe énoncé. Mais ce choix pourra également avoir des conséquences importantes, étant entendu qu'en pratique, une grande tolérance dans l'utilisation du système d'information pourra mener plus facilement à des abus et qu'au contraire, une vision trop stricte des possibilités offertes aux salariés dans l'utilisation des ressources informatiques, mis à part le fait qu'elle sera peu réaliste, comportera un risque non négligeable de requalification *a posteriori* par le juge, en cas de contentieux devant les tribunaux.

Par exemple, le fait d'interdire ou non l'usage privé de la messagerie électronique devra être non seulement harmonisé avec les principes d'organisation de l'entreprise, mais également prendre en compte l'évolution de la jurisprudence. Si une rédaction est plus stricte que l'interprétation des tribunaux, en cas de contentieux, elle risque d'être considérée comme nulle par le juge, voire d'entraîner la nullité de l'intégralité de la charte. Pour autant, une utilisation à titre personnel sans aucune réserve augmentera, par exemple, les risques de dissémination d'informations confidentielles hors de l'entreprise.

Dans le chapitre III, les rédacteurs du présent guide se sont efforcés de choisir des exemples de rubriques plus ou moins souples, qui pourront être adaptés à l'approche et à l'organisation de l'entreprise, tout en mesurant les risques associés à chaque niveau de rédaction, de l'interdiction totale à une approche plus ouverte.
Le lecteur trouvera dans l'annexe 2 un panorama de la jurisprudence afférente à l'utilisation des ressources informatiques et des moyens de communication électronique dans l'entreprise.

II.6. CHOIX DU VOCABULAIRE

De manière globale, la rédaction sera volontairement détaillée ou générale. Cette seconde possibilité engendre une perte de précision afin cependant de s'adapter avec souplesse aux évolutions technologiques ou terminologiques et de ne pas avoir à modifier la charte trop souvent.

Le choix du vocabulaire sera adapté aux objectifs de la charte et à la terminologie spécifique de l'entreprise. Il pourra être précis (micro-ordinateur, messagerie électronique) ou volontairement générique (système d'information, ressources informatiques).

II.7. INFORMATION SUR LES MOYENS DE CONTROLE DES UTILISATEURS

Au-delà de la réglementation spécifique aux traitements informatiques des données à caractère personnel, l'utilisateur et les instances représentatives des salariés devront être informés des autres moyens techniques pouvant éventuellement porter atteinte à la vie privée, comme la vidéosurveillance par exemple.

Pour certaines fonctions spécifiques de l'entreprise (ex : salle des marchés), des outils de contrôle particuliers peuvent être mis en œuvre, par exemple des enregistrements téléphoniques. Dans ce cas, l'ensemble du personnel soumis à ce contrôle doit en être informé, de même que de la durée de conservation des enregistrements.

II.8. SENSIBILISATION – COMMUNICATION

Pour être efficace, on recherche souvent à ce que la charte obtienne l'adhésion des salariés, bien qu'un tel document ne soit, à tort ou à raison, jamais bien accueilli dans une entreprise. Aussi, celle-ci doit être élaborée dans un souci de sensibilisation et de pédagogie en justifiant les mesures parfois contraignantes susceptibles d'être imposées. Les vulnérabilités doivent être présentées, en considérant notamment que la richesse de l'entreprise dépend également de la protection de ses valeurs (outil, savoir-faire et connaissances techniques de l'ensemble des salariés, ce que l'on a pu appeler son « patrimoine informationnel »), et de sa réputation (responsabilité civile et pénale des dirigeants ou de la personne morale).

La réussite de la charte et son opposabilité seront souvent d'autant plus forts que celle-ci aura été présentée et commentée aux salariés afin de préciser l'engagement de chacun.

De telles mesures devront s'inscrire dans une logique de partenariat de tous les utilisateurs.

III. RECOMMANDATIONS SUR LE CONTENU DE LA CHARTE ILLUSTREES D'EXEMPLES

III.1. REGLEMENTATION

La responsabilité encourue par l'employeur l'incite à avertir les utilisateurs de leur engagement à respecter la réglementation, même si cet aspect transparaît déjà dans d'autres rubriques. Comme il ne semble pas envisageable de citer ici l'essentiel des règles civiles et pénales applicables, la rédaction peut rester générale :

> *« Les collaborateurs s'engagent à respecter la réglementation applicable dans le cadre de l'utilisation des ressources informatiques. »*

On peut aussi faire référence aux informations concernant la réglementation applicable qui seraient rendues accessibles grâce aux ressources informatiques mises à la disposition des utilisateurs :

> *« L'usage des ressources informatiques mises à la disposition des utilisateurs doit être conforme à la réglementation en vigueur sur le territoire d'établissement de leur employeur et*

sur le territoire sur lequel ils les utilisent. Ils seront invités à suivre la formation (référence) organisée par l'entreprise et à consulter le site Intranet (adresse) ».

III.2. VIE PRIVEE RESIDUELLE

Les ressources informatiques sont mises à la disposition des utilisateurs pour un usage professionnel correspondant à la réalisation des missions et des objectifs de l'entreprise, dans le cadre de la législation applicable, du statut du personnel, du règlement intérieur et des textes qui y sont formellement attachés.

> *« L'utilisateur est responsable de l'usage qu'il fait des ressources informatiques de l'entreprise dans l'exercice de sa fonction. Il doit en réserver l'usage au cadre de son activité professionnelle. »*

Selon les entreprises, un usage personnel, raisonnable (limité dans sa fréquence comme dans sa durée, ne perturbant pas les activités professionnelles), des ressources informatiques peut toutefois être admis, comme il l'était souvent déjà pour le téléphone. La jurisprudence est encore partagée quant à la reconnaissance d'un droit d'usage privé à l'utilisateur de ces outils (voir en annexe 2).
Le principe n'en demeure pas moins que « *les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel* » (Cour de cassation, 18 octobre 2006).

Les exemples ci-dessous insistent sur la responsabilité de l'utilisateur :

> *« Les ressources informatiques sont mises à la disposition des utilisateurs à des fins professionnelles. Un usage à des fins personnelles de ces ressources est toléré lorsqu'il s'inscrit dans le cadre des nécessités de la vie privée. Dans ce cas, l'utilisation des ressources informatiques de l'entreprise à des fins privées pourra conduire l'utilisateur à assumer l'entière responsabilité pénale et civile de l'utilisation qu'il fera des ressources informatiques et notamment des moyens de connexion. »*
> *« Les moyens informatiques mis à disposition ne doivent pas être utilisés pour des activités lucratives susceptibles d'engager la responsabilité de l'entreprise. »*

Un autre mettant l'accent sur les limites du raisonnable :

> *« L'usage de la messagerie, du téléphone et du fax sont réservés à des fins strictement professionnelles sauf tolérance à titre exceptionnel, sous réserve qu'il n'affecte ni la tenue du poste de travail ni le trafic des messages professionnels.*
> *De même l'usage de l'Internet est réservé à des fins strictement professionnelles mais une consultation pour un motif personnel est tolérée si elle demeure occasionnelle, de courte durée, se limite à des sites Internet dont le contenu n'est pas contraire à l'ordre public ou aux bonnes mœurs, si elle n'affecte pas la tenue du poste de travail, la sécurité et le bon fonctionnement des systèmes d'information et ne met pas en cause l'intérêt et la réputation de l'entreprise.*
> *En tout état de cause l'utilisateur se gardera de commettre des actes, qu'ils soient à caractère privé ou professionnel, qu'il s'interdirait dans le cadre de sa vie privée. »*

Dans ce cadre, certains documents sont de nature « privée », quelle que soit leur forme, s'ils ont été créés par un utilisateur pour son usage exclusif. L'entreprise doit respecter les dispositions légales en matière de protection de la vie privée et des libertés individuelles.

> *« Les administrateurs peuvent être amenés, à titre exceptionnel et à des fins de sécurité ou d'administration du système, à accéder avec des procédures définies au contenu de fichiers, y compris les documents privés, enregistrés sur les supports de stockage. Il leur est interdit de les divulguer, de les utiliser ou de les modifier et, sauf impératif technique ou de sécurité majeur, de les supprimer. »*

Par ailleurs, l'utilisateur doit respecter les règles posées quant à la création de tels documents, si l'employeur en a accordé la possibilité et dans les limites qu'il a fixées.

> *« Les interventions techniques sont menées en tant que de besoin et ne sauraient en aucun cas être différées ou aménagées du fait de la tolérance d'un usage privé des ressources. L'entreprise ne prend, en conséquence, aucun engagement en matière d'intégrité, de permanence et de disponibilité des documents privés. Il appartient aux utilisateurs de les gérer et d'en assurer la sauvegarde. »*

III.3. CONFIDENTIALITE

La définition de la notion de confidentialité des informations du système d'information peut être rappelée dans la charte. La confidentialité est « *la tenue secrète des informations avec accès aux seules entités autorisées* » (Glossaire du *Livre blanc sur la sécurité des systèmes d'information dans les établissements de crédit,* 1996).

> *« Chaque utilisateur est responsable pour ce qui le concerne du respect du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. »*

> *« Il doit respecter le niveau de classification défini et rattaché à chaque information et les mesures de sécurité associées (avec un renvoi approprié aux documents existants dans l'entreprise). »*

> *« Chaque utilisateur doit être vigilant quant au risque de divulgation ou de publication des informations qu'il utilise dans l'exercice de ses fonctions particulièrement lorsque sont utilisés des moyens de communication électronique. Les règles de confidentialité ou d'autorisation préalable avant diffusion externe ou publication sont applicables quel que soit le support de communication utilisé. »*

> *« Chaque utilisateur doit être vigilant sur le risque de divulgation dans le cadre d'utilisation d'outils informatiques (micro-ordinateurs portables, assistants numériques personnels [PDA]…) dans les lieux autres que ceux de l'entreprise (hôtels, lieux publics, transports…). »*

III.4. SECURITE DU SYSTEME D'INFORMATION

Il s'agit là de règles très générales portant sur l'engagement de chaque utilisateur de ne pas nuire à la sécurité du système d'information :

> *« L'utilisateur s'engage à ne pas compromettre l'accès aux données et applications que ce soit de manière physique ou logicielle, à ne pas compromettre leur intégrité ou leur confidentialité. Il s'engage notamment à ne contourner aucun des systèmes de sécurité mis en œuvre dans l'entreprise. »*

III.5. MOYENS D'AUTHENTIFICATION

Divers moyens d'authentification sont possibles : mot de passe, badge, biométrie. Dans tous les cas, l'authentification est la clé de la confidentialité. Il importe donc que la charte précise un certain nombre de règles :

> *« Les moyens d'authentification sont personnels et confidentiels, ils ne doivent pas être communiqués ou partagés par plusieurs utilisateurs. »*

III.5.1. Obligation de protection des authentifiants

> *« Chaque utilisateur doit assurer la protection des moyens d'authentification (badges, mots de passe statiques, cartes délivrant des mots de passe à usage unique, certificats…) qui lui ont été affectés sur tous les équipements mis à sa disposition y compris les équipements mobiles. »*
>
> *« Il doit prendre toutes les précautions nécessaires pour en préserver la confidentialité. »*

III.5.2. Interdiction des partages et délégations des authentifiants

> *« Aucun utilisateur ne doit faire usage des moyens d'authentification ou des habilitations d'un tiers, sauf en cas de force majeure et/ou de demande formelle de sa hiérarchie. »*

Ou encore :

> *« L'utilisateur ne doit pas se servir, pour accéder au système d'information de l'entreprise, d'un autre compte que celui qui lui a été attribué. De même il s'engage à ne pas déléguer les droits d'utilisation des systèmes d'information qui lui sont attribués, sauf lorsque les nécessités du service l'imposent et après accord formalisé par un écrit de sa hiérarchie. »*

Et aussi :

> *« L'utilisateur ne doit pas communiquer ses moyens d'authentification ou les prêter à une tierce personne sauf en cas de demande formelle de sa hiérarchie. »*

III.5.3. Respect des règles sur les mots de passe

Des règles permettent d'assurer la robustesse des mots de passe, elles doivent être respectées :

> *« Les mots de passe doivent être choisis et modifiés régulièrement en fonction des règles de sécurité mises en place dans l'entreprise, qui doivent être respectées par tous. »*
>
> *« Pour tous les systèmes d'authentification l'utilisateur doit respecter les règles de délivrance et de mise à jour prévues dans l'entreprise. »*

III.6. GESTION DU SYSTEME D'INFORMATION

Si l'entreprise a une organisation structurée de la gestion de son parc matériel et logiciel, il peut être important de le préciser :

> *« Les autorisations d'accès aux ressources informatiques, le choix et l'installation de matériels et de logiciels sont effectués par les services de l'entreprise qui en sont responsables. Elles ne relèvent pas des utilisateurs. »*

III.7. INCIDENTS

La remontée des incidents peut jouer un rôle crucial dans la rapidité de détection et de réaction à un incident :

> *« Chaque utilisateur doit rendre compte le plus rapidement possible des incidents ou anomalies qu'il constate dans tous les domaines liés à l'utilisation des ressources informatiques ou des moyens de communication électronique (authentification, identification des expéditeurs ou de fichiers joints suspects, tentative d'intrusion, infection par un virus…) selon les procédures en vigueur dans l'entreprise. »*

Une autre formulation possible sur l'engagement de signalement de toute atteinte à la sécurité du système d'information serait :

> *« L'utilisateur signale sans délai à … tout constat, tentative ou soupçon d'accès non autorisé ou de compromission de l'intégrité ou de la confidentialité des données et applications de l'entreprise. »*

III.8. INTEGRITE DU SYSTEME D'INFORMATION

III.8.1. Intégrité du poste de travail

La charte contiendra au minimum l'interdiction de principe :

> *« Il est interdit de modifier la configuration matérielle ou logicielle d'un poste de travail.»*

On peut l'illustrer par des exemples, à adapter selon les particularités de l'entreprise :

> *« Il est notamment interdit d'y connecter un modem, d'y activer le partage de ressources, d'y désactiver l'écran de veille, d'y installer tout logiciel qui ne serait pas fourni par l'entreprise. »*

Ces dispositions pourront être utilement complétées par les exemples suivants :

> *« Il est interdit de connecter au poste de travail tout dispositif mobile qui n'aurait pas été agréé par l'entreprise. C'est notamment le cas des périphériques de stockage externe : clé USB, graveur de CD ou DVD, baladeur MP3, etc. »*

Lorsque l'entreprise procède à une sécurisation stricte (durcissement) des configurations, on peut souhaiter informer l'utilisateur de ce verrouillage :

> *« À des fins de sécurité, la configuration du poste de travail peut être verrouillée par l'entreprise. »*

Et l'on peut surtout formuler l'interdiction générale suivante :

> *« Il est interdit de contourner les dispositifs de protection du poste de travail. »*

III.8.2. Intégrité du réseau

Au-delà du poste de travail, c'est de l'intégrité de la partie du système d'information accessible au salarié qu'il faudrait parler. Par exemple :

« Il est interdit de connecter au réseau de l'entreprise tout élément qui n'aurait pas été autorisé par l'entreprise, et notamment un ordinateur, un périphérique, une borne d'accès de réseau sans fil (Wi-Fi, etc.). »

III.8.3. Intégrité du système d'information

Une règle générale peut être formulée :

« L'utilisateur n'introduit dans le système d'information de l'entreprise aucune donnée non répertoriée ou approuvée par l'entreprise. Il ne tentera pas d'y accéder sans autorisation et ne supprimera aucun fichier ou donnée (de tiers ou fichiers systèmes) pouvant mettre en cause l'intégrité du système d'information ou l'activité de l'entreprise. »

Elle peut être précisée ainsi pour donner un exemple concret :

« Il est notamment interdit de copier sur le poste de travail tout fichier d'origine incertaine. »

« Il ne peut pas installer sur les serveurs de ressources partagées ou sur son poste de travail des logiciels susceptibles de contourner, d'affaiblir ou de perturber la sécurité ou les performances du système d'information.»

III.9. SECURITE DU POSTE DE TRAVAIL

III.9.1. Usage des logiciels de sécurité du poste de travail

L'usage de logiciels assurant la sécurité du poste de travail peut figurer dans la charte, avec notamment l'interdiction de les supprimer ou de les contourner (ce qui est un cas particulier par rapport aux règles évoquées dans le chapitre précédent sur l'intégrité du poste de travail).

« Chaque utilisateur prend et respecte toute mesure visant à éviter le chargement ou téléchargement d'un programme malveillant ; il est responsable de l'utilisation des programmes de sécurité de son poste de travail, qui ne doivent en aucun cas être désactivés. »

Afin de bien être compris, on peut nommer les principaux logiciels de ce type utilisés aujourd'hui (le principe général étant fixé ci-dessus, la charte conservera son actualité même en cas d'évolution de la liste ci-dessous, qui est fournie à titre d'exemple pédagogique) :

« C'est notamment le cas de l'antivirus, du pare-feu (firewall), de l'antispyware. »

Lorsque l'utilisateur doit mettre à jour lui-même l'antivirus (ce qui peut être le cas dans certaines entreprises, en particulier pour les utilisateurs de portables), il peut être utile de préciser :

« Lorsque l'employeur lui confie la mise en œuvre de mesures de sécurité sur son poste de travail (par exemple la mise à jour de l'antivirus, du pare-feu ou de l'antispyware), l'utilisateur s'y conforme en respectant les modalités (notamment la fréquence) qui lui sont prescrites. »

Attention : l'entreprise ne peut logiquement pas prévoir de mises à jour du poste de travail en dehors des horaires de travail si elle n'accepte pas l'usage privé qui serait fait de celui-ci.

III.9.2. Mesure à prendre contre les programmes malveillants

Le point faible dans la protection antivirale restant le facteur humain, il est bon d'exiger de l'utilisateur un comportement responsable :

> *« L'utilisateur s'engage à détruire immédiatement tout document reçu (par messagerie, disquette, clé USB, CD/DVD-ROM, ou tout autre moyen) de provenance inconnue ou sans rapport avec son activité professionnelle. »*

III.10. MODALITES D'EXPRESSION DES UTILISATEURS

Il semble utile de rappeler que les droits d'expression des utilisateurs sont exercés dans le respect de l'image de l'entreprise et des lois en vigueur.

> *« L'utilisateur ne doit adresser à l'intérieur ou à l'extérieur de l'entreprise aucun message susceptible de porter atteinte aux intérêts ou à l'image de l'entreprise, de ses dirigeants, de ses clients, ou de l'un de ses salariés. Il ne pourra être amené à s'exprimer au nom et pour le compte de l'entreprise que sur autorisation expresse des dirigeants de ladite entreprise. »*

La formulation suivante rappelle à l'utilisateur que sa responsabilité, ainsi que celle de l'employeur, sont engagées par le contenu des messages électroniques, comme de tout média :

> *« L'accès aux ressources informatiques et notamment aux moyens de communication électronique est mis à disposition des utilisateurs à des fins professionnelles.*
> *Sauf restrictions particulières définies par la hiérarchie, cet accès peut servir aux relations contractuelles ou commerciales à titre professionnel pour lesquelles il convient de respecter les règles suivantes :*
>
> - *lorsqu'ils peuvent engager l'entreprise, les échanges utilisant des moyens de communication électronique doivent être validés et approuvés au niveau hiérarchique nécessaire ;*
> - *les circuits habituels de relecture et d'approbation par les personnes dûment habilitées doivent être respectés avant d'émettre un message. »*

> *« L'utilisateur ne doit jamais écrire un message électronique qu'il s'interdirait d'exprimer oralement ou par un autre moyen (courrier, télécopie, etc.), les propos transmis par ce biais pouvant engager la responsabilité de leur auteur et de l'entreprise.*
> *Il doit utiliser avec discernement les listes de diffusion personnelles ou collectives et éviter l'envoi de copies à un nombre injustifié de destinataires. »*

Les conditions d'expression personnelle s'inscrivent également dans l'environnement réglementaire et les règles d'usage raisonné des outils. Par exemple :

> *« Il est interdit de transmettre, retransmettre ou publier des messages contribuant à un harcèlement sexuel ou moral, menaces ou insultes et de manière générale contraires aux lois en vigueur. »*

On peut également compléter avec cette disposition :

> *« L'utilisateur ne doit pas transmettre des messages de type canulars (hoaxes en anglais) : chaînes du bonheur, fausses alertes, rumeurs (informations non vérifiées susceptibles d'induire quelqu'un en erreur). »*

III.11. CONTROLE DE L'ACCES A L'INTERNET

III.11.1. Interdiction d'accès à certains sites Web

Il est nécessaire de rappeler qu'il est interdit de consulter certains sites.

L'interdiction peut se limiter explicitement à ce qui est pénalement répréhensible, en reprenant par exemple une formulation de la Loi pour la Confiance dans l'Economie Numérique (LCEN) :

> *« Il est interdit de consulter des sites Internet relevant de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ou de la pornographie enfantine. »*

La législation pouvant évoluer, ce qui est permis aujourd'hui peut être illicite demain (ou l'inverse), il peut donc être conseillé d'interdire tout site illicite. Par exemple :

> *« Il est interdit de consulter des sites Internet illicites ou contraires au respect de la dignité de la personne humaine. »*

L'interdiction peut être plus vaste et ne pas se limiter à ce qui est illicite, mais englober ce qui est « contraire aux bonnes mœurs » (notion évolutive et même subjective, qui offre au juge une grande marge de manœuvre, mais qui reflète le consensus d'une époque ; par exemple, la pornographie enfantine est illicite, alors que la pornographie adulte n'est pas illicite, mais bien contraire aux bonnes mœurs) :

> *« La consultation doit se limiter à des sites Internet dont le contenu n'est pas contraire à l'ordre public ou aux bonnes mœurs. »*

Enfin, on peut trouver aussi des formulations extensives, très détaillées, comme celle-ci, qui étend le champ d'interdiction aux contenus portant atteinte à l'image de marque de l'entreprise :

> *« Il est notamment interdit, lors de l'utilisation des moyens de communication électronique fournis par l'entreprise, de rechercher, visualiser, télécharger, transmettre ou conserver des contenus à caractère pornographique, pédophile, raciste, xénophobe, diffamatoire, portant atteinte au respect de la personne humaine et à sa dignité, incitant à la commission d'un délit ou d'un crime, contraires à l'ordre public ou aux bonnes mœurs, attentatoires à l'image de marque interne ou externe de l'entreprise. »*

Autre exemple explicite (notons qu'il indique que « *les lois […] doivent être respectées* » ; il n'interdit donc pas les sites contraires aux bonnes mœurs, mais uniquement les sites illicites) :

> *« L'utilisation de l'Internet à des fins commerciales en vue de réaliser des gains financiers ou de soutenir des activités lucratives est strictement interdite.*
> *Les lois relatives aux publications à caractère injurieux, raciste, sexiste, pornographique, pédophile doivent être respectées. La recherche, le téléchargement, la transmission ou le stockage de ce type de documents ne sont pas autorisés. »*

Dans l'exemple suivant, le but est d'interdire la consultation de sites dangereux pour le système d'information même de l'entreprise, afin que ceux-ci ne soient pas utilisés par des pirates informatiques pour infester un réseau ou largement propager des logiciels malveillants (« *malwares* »). On peut imaginer également vouloir limiter la consultation de sites incitant à transmettre, de façon chiffrée par exemple, des informations confidentielles à l'extérieur de l'entreprise.

« Il est interdit de consulter des sites dont l'utilisation pourrait comporter un risque pour le système d'information de l'entreprise en contournant les dispositifs de protection technique ou de confidentialité des informations mis en place.
En cas d'abus, l'accès à Internet pourra être restreint ou clos. »

III.11.2. Le filtrage déontologique

Le filtrage déontologique, c'est-à-dire un système automatique d'interdiction d'accès à certaines catégories de sites, le plus souvent accompagné de l'enregistrement d'un certain nombre de données relatives aux connexions aux sites, doit, lorsqu'il existe, impérativement faire l'objet d'une information des utilisateurs.

La formulation peut être fort concise :

« Des mécanismes de filtrage peuvent être mis en place pour interdire l'accès à certains sites. »

En ce qui concerne la surveillance du trafic, et afin d'être conforme à l'esprit de la loi sur l'informatique et les libertés, il convient d'être précis tant sur les finalités des contrôles que sur la durée de conservation des informations enregistrées.

Exemple sur les finalités :

« À des fins de statistiques, de qualité de service et de sécurité, le trafic Internet est sujet à une supervision et à des vérifications et contrôles réguliers par l'entreprise, dans les limites prévues par la loi. »

Exemple complémentaire sur la nature des informations conservées et la durée de cette conservation :

« Peuvent être également mis en place des contrôles a posteriori portant sur la volumétrie des connexions à des sites Internet : relevé des sites les plus visités, des utilisateurs ayant généré le plus de requêtes (hits), relevé, pour chacun des utilisateurs les plus importants, des durées de connexion et des sites les plus fréquentés. »
« Ces informations sont remises confidentiellement au déontologue de l'unité. Elles peuvent être conservées un an (sous réserve de dispositions légales ou réglementaires impliquant une durée de conservation différente). »

III.11.3. L'interdiction d'accéder aux sites payants

Une mention particulière est faite par certaines entreprises concernant les sites payants.
Elle peut être axée sur le risque d'engagement financier de l'entreprise :

« Il est interdit à l'utilisateur d'engager financièrement l'entreprise par la consultation de sites payants à titre privé. »
« Lorsqu'il doit consulter des sites payants à titre professionnel, l'utilisateur doit y être dûment autorisé par sa hiérarchie. »

Ou plus impérative :

« Il est interdit d'accéder à des sites payants, de participer à des jeux en ligne (et notamment des jeux d'argent), d'entretenir sur l'Internet des relations commerciales à titre privé. »

III.11.4. L'interdiction de réaliser des sites Internet

L'arrêt « Escota » précité, rendu par la Cour d'appel d'Aix-en-Provence a confirmé un jugement du Tribunal de grande instance de Marseille qui avait déclaré une société responsable, en sa qualité de commettant, des agissements de l'un de ses collaborateurs ayant utilisé l'infrastructure d'accès à l'Internet pour réaliser un site personnel contrefaisant une marque et tenant des propos injurieux à son égard. Le premier jugement faisait en particulier valoir que, dans la note du DRH de l'entreprise autorisant un usage personnel raisonnable de l'Internet, « *aucune interdiction spécifique n'était formulée quant à l'éventuelle réalisation de sites Internet ou de fourniture d'informations sur des pages personnelles.* ».

Cela peut inciter à inclure dans la charte une interdiction explicite de création ou de mises à jour de sites :

> *« En dehors du cadre strictement professionnel, il est interdit de créer ou mettre à jour, au moyen de l'infrastructure d'accès à l'Internet fournie par l'entreprise, tout site Internet (notamment pages personnelles, journal personnel en ligne [blogue, blog, weblog], site Web collaboratif [sites Wiki]). »*

III.12. MESSAGERIE (MESSAGERIE ELECTRONIQUE ASYNCHRONE)

Plusieurs points sont à considérer. Tout d'abord, il convient de trancher le point de savoir si l'on souhaite accorder ou non un usage privé des outils de messagerie de l'entreprise (*cf. supra* : Vie privée résiduelle).

Cette faculté d'usage privé est très discutée et fait l'objet de décisions de jurisprudence contradictoires (voir annexe 2). Précisons que la doctrine juridique paraît majoritairement soutenir la position en faveur de la reconnaissance d'un usage privé.

Ensuite se pose la difficulté de la distinction, en pratique, du flux des messages privés de celui des messages professionnels. Il convient de réfléchir à la mise en place, à cette fin, de procédures d'archivage, de reprise sur incident et de conservation à des fins de preuve qui intègrent cette distinction et permettent d'appliquer les règles éventuellement différentes qui auraient été adoptées par l'entreprise.

Enfin, il faut relever que la mise en place de procédures de filtrage de spams ou de messages infectés par des virus ou comportant des logiciels malveillants, pourrait conduire à l'élimination de messages au contenu privé. Prévenir l'utilisateur de l'application de ces règles et des conséquences qu'elles peuvent engendrer (au regard de leur indéniable apport pratique) permet logiquement de se mettre à l'abri d'un risque très théorique de poursuite pour destruction de correspondance.

Dans ce contexte, il paraît opportun de prévenir l'utilisateur que :

> *« Les procédures de contrôle (filtrage antiviral, antispam…) seront appliquées à tous les messages. »*

III.12.1. Cas 1 : usage professionnel exclusif

Sous les réserves énoncées ci-dessus, cette formulation prévoit l'interdiction de tout usage privé.

« L'utilisateur ne doit employer l'accès à Internet, la messagerie ou plus généralement l'ensemble des ressources informatiques mises à sa disposition par l'employeur, que dans le cadre exclusif de son activité professionnelle. »

III.12.2. Cas 2 : usage privé généralisé toléré

Cet exemple prend en compte l'usage privé et se base sur le principe de labellisation des messages, c'est-à-dire en l'occurrence, une identification permettant de faire apparaître clairement la nature personnelle du message.

« Par exception, un usage raisonnable, à titre privé, de l'accès à l'Internet, de la messagerie ou plus généralement de l'ensemble des ressources informatiques mises à sa disposition par l'employeur, est toléré dans le cadre des nécessités de la vie courante et familiale. Cet usage privé doit être limité et de courte durée afin de ne pas affecter l'exploitation normale du système informatique de l'employeur. »

« S'il fait usage de cette faculté, l'utilisateur devra (à préciser lors de la rédaction de la charte un type de labellisation). *Il devra également, lorsqu'il communique son adresse électronique à des correspondants privés, leur indiquer cette règle. »*
« Les messages comportant … (labellisation à préciser lors de la rédaction de la charte) *pourront être conservés en tout état de cause par l'employeur pendant une durée de… et être utilisés dans le cadre de procédures de contrôle interne ou de preuve des échanges commerciaux effectués. »*

« Seront notamment considérés comme fautifs ou abusifs les agissements suivants :

- *l'échange d'informations confidentielles sans protection adéquate et autorisée,*
- *la redirection de sa messagerie vers une messagerie personnelle,*
- *l'échange de messages à caractère xénophobe, raciste, négationniste ou des contenus pornographiques, notamment mettant en scène des personnes mineures,*
- *l'échange de messages sous un identifiant différent de celui de l'utilisateur,*
- *d'une manière générale, l'utilisation de la messagerie électronique dans des conditions susceptibles de porter atteinte à l'image, à la réputation ou à la sécurité d'autrui ou de l'employeur ou au bon fonctionnement du système d'information de l'entreprise (taille des messages et contenu…), etc. »*

III.12.3. La solution Webmail

Certaines entreprises ont retenu une autre solution pour l'usage privé de la messagerie : les services de messagerie en ligne (Webmail).

« L'utilisateur ne doit employer la messagerie, mise à sa disposition par l'employeur, que dans le cadre exclusif de son activité professionnelle. L'utilisateur devra, s'il souhaite envoyer des messages électroniques à titre privé, créer un compte sur les services de messagerie en ligne suivants … qui lui seront accessibles par le biais de la connexion à l'Internet de son poste de travail. Lors de ces consultations, l'utilisateur devra respecter les règles de consultation de l'Internet (usage limité…). »

D'autres entreprises jugent au contraire que l'utilisation de Webmails constitue un risque en matière de sécurité des systèmes d'information (principalement en raison de la potentialité de transfert de pièces jointes infectées). Ce risque peut être couvert par un filtrage antivirus des flux Web, mais, si ce

n'est pas le cas, le passage par un service Webmail affranchit l'utilisateur des contrôles antivirus qui auraient été effectués en messagerie classique sur les serveurs de messagerie de l'entreprise.

> *« Afin de garantir la sécurité des ressources informatiques de l'entreprise, l'utilisation de services de courriers électronique en ligne (de type Webmail) est interdite. »*

Le cas échéant, il conviendra de coupler cette interdiction avec un filtrage des URL des services Webmail (*cf. supra* III.11.).

III.13. MESSAGERIE INSTANTANEE ET TELEPHONIE SUR IP

Ici encore doivent être considérés les points mentionnés concernant la messagerie « classique », avec une différence : on peut imaginer permettre une utilisation à titre privée de la messagerie « classique » et limiter l'utilisation de la messagerie instantanée au cadre professionnel.

Autre façon d'assurer cette limitation : interdire l'installation de tels logiciels sur les postes, dans le cadre de dispositions *ad hoc*. Une telle restriction est justifiée par les impératifs de sécurité auxquels doit faire face l'entreprise dans le cadre de la gestion de son parc informatique.
Il faudra, par ailleurs, afin de limiter pleinement l'accès à ce type de services, organiser le filtrage des URL de ces services dans les cas ou ceux-ci ne requièrent pas l'installation d'un logiciel client.

> *« L'usage d'outils dits de « messagerie instantanée » et de téléphonie sur IP est strictement réglementé pour des raisons tenant aux risques en matière de sécurité que ces outils génèrent particulièrement. Compte tenu de la tolérance d'utilisation de la messagerie électronique classique à titre privée, l'usage de toute messagerie instantanée ou de service de téléphonie sur IP, lorsque l'utilisation d'un de ces outils a été spécifiquement autorisée par la hiérarchie, est donc strictement réservé à des fins professionnelles. En application des dispositions réglementaires spécifiques…, le contenu de ces messages sera conservé par l'employeur pendant une durée de..., et pourra être utilisé dans le cadre de procédures de contrôle interne ou de preuve des échanges commerciaux effectués. »*

Principe d'interdiction avec exception :

> *« L'utilisation d'outils dits de « messagerie instantanée » et de services de téléphonie sur IP internes ou externes de type* (à préciser lors de la rédaction de la charte) *n'est pas autorisée. Des dérogations exceptionnelles dans le cadre de l'activité professionnelle peuvent être données avec l'autorisation préalable d'un représentant habilité de… À ce titre, l'enregistrement des communications effectuées au travers de ces services peut être alors demandé selon l'activité de l'utilisateur. »*

III.14. FORUMS

L'accès et la participation à des forums de discussion pourront faire l'objet d'une interdiction :

> *« Il est interdit de consulter ou de participer à des forums de discussion. »*

Ou bien être soumis à certaines conditions d'utilisation :

> *« L'utilisateur doit exercer une vigilance toute particulière à l'égard du contenu des échanges et il lui est interdit, lors de l'utilisation des comptes et infrastructures fournies par l'entreprise, de participer à des forums de discussions sur Internet, une liste de diffusion ou un service d'échange de fichiers, sauf si ceux-ci sont de nature professionnelle ou à condition de s'y exprimer à titre personnel avec réserve, sans y laisser son adresse. »*

III.15. STOCKAGE DE DONNEES

Que veut-on encadrer ? Que veut-on limiter ? Que veut-on permettre ? L'entreprise doit se poser ces questions, définir une organisation. En conséquence les formulations peuvent être très différentes selon le but recherché.

III.15.1. Consignes de stockage

Le premier point peut concerner le respect des consignes de stockage des données essentiellement orientées vers la garantie de leur disponibilité (par exemple, l'interdiction d'utilisation du disque dur de la station de travail, l'obligation d'utiliser certains espaces de stockage sur serveurs de fichiers faisant l'objet de sauvegardes, etc.)

> *« L'utilisateur doit respecter les consignes qui lui sont communiquées en matière de stockage et de sauvegarde des données. »*

Il semble opportun de rappeler ici que l'utilisateur est tenu de garantir la disponibilité des données stockées sur son poste de travail. Il ne doit pas mettre en place de mesures en restreignant l'accès autres que celles prévues par l'entreprise pour garantir la confidentialité de l'information. La jurisprudence la plus récente rappelle sur ce point que constitue une faute le fait pour le salarié de rendre inaccessible l'accès aux fichiers de son poste de travail (tant professionnels que personnels), en l'occurrence par l'emploi de procédés de chiffrement (Cour de cassation, 18 octobre 2006).

III.15.2. Protection de la confidentialité des données

On peut également vouloir rappeler les règles de confidentialité (cf. *supra*) et restreindre la diffusion d'informations protégées :

> *« L'utilisateur veillera particulièrement à respecter les règles sur la confidentialité décrites à l'article… et à ne pas disséminer en dehors de l'entreprise des documents auxquels il a eu accès dans le cadre professionnel, notamment par voie de stockage sur des supports acquis à titre personnel ou via des transferts de fichiers… »*

III.15.3. Les données privées

Pour un usage privé (*cf. supra* Vie privée résiduelle) raisonnable mais limité :

> *« L'utilisateur, s'il utilise les ressources informatiques mises à sa disposition par l'employeur pour stocker ou utiliser des données à des fins extraprofessionnelle, devra veiller à n'en faire qu'une utilisation raisonnable et limitée, notamment en volume. En tout état de cause, il devra s'assurer de la parfaite innocuité de ces fichiers pour le système d'information de l'employeur, il ne devra pas perturber ou limiter les capacités techniques mises à sa disposition à une fin professionnelle et devra respecter l'ensemble des dispositions réglementaires applicables aux contenus stockés ou utilisés (droit d'auteur, droit à l'image…). Ces fichiers ne doivent en aucun cas être susceptibles de porter atteinte à l'image de l'entreprise. »*

Pour un usage privé raisonnable mais limité avec fortes possibilités d'action pour l'entreprise (il convient de préciser qu'une telle procédure serait cependant susceptible d'être remise en cause par les tribunaux en cas de litige), la formulation précédente peut être complétée par :

> *« En cas de suspicion de non-respect de ces dispositions, l'employeur pourra notamment retirer et/ou effacer les contenus stockés sans avoir à en avertir préalablement l'utilisateur. »*

Enfin, on peut envisager une interdiction totale, étant entendu que l'on peut sérieusement douter de l'accueil que pourraient réserver les juridictions à un tel principe encore plus strict que celui décrit plus haut. La conséquence d'une telle formulation risquerait d'être l'invalidation de l'ensemble de la disposition, ce qui serait contraire au but recherché :

> *« L'utilisateur ne devra importer, stocker ou utiliser aucune donnée à des fins extraprofessionnelles sur les infrastructures techniques de l'employeur. »*

III.16. INFORMATIQUE ET LIBERTES

L'employeur peut rappeler les obligations imposées par la réglementation en la matière (loi du 6 janvier 1978 modifiée), c'est-à-dire déclarer le traitement auprès de la CNIL avant sa mise en œuvre, ne pas en détourner les finalités et respecter les obligations liées à la collecte des données, ainsi qu'à leur conservation, confidentialité, sécurité et à l'information des utilisateurs de leur droit d'accès.

Cela vise les traitements de données à caractère personnel (fichier de clients, fournisseurs, etc.) que l'utilisateur aurait pu constituer à l'exception de son carnet d'adresse personnel.

> *« Avant de mettre en œuvre un traitement de données à caractère personnel, l'utilisateur s'engage à consulter la procédure …* (référence) *ou le service …* (à désigner), *afin de se conformer aux dispositions de la réglementation en la matière. »*

III.17. CONTRÔLES ET UTILISATIONS PAR L'EMPLOYEUR DES DONNEES COLLECTEES

Afin de préciser ce que l'employeur pourra faire des données collectées ainsi que la manière selon laquelle il pourra procéder au contrôle, plusieurs clauses *ad hoc* devront être ajoutées.

Exemple 1 :

> *« Pour des raisons de gestion technique, de maintenance, de planification des ressources matérielles ou logicielles et de sécurité de l'ensemble des ressources informatiques, l'administration, la surveillance et le contrôle de l'utilisation des moyens informatiques et de communication électronique relèvent, dans le respect de la réglementation, de services de l'entreprise expressément désignés selon les procédures suivantes… »*
>
> *« Le contrôle de tout acte d'utilisation comprend la possibilité d'accéder et d'éditer des états et journaux de bord traitant de données figurant sur les postes individuels, sur le réseau et sur les ressources informatiques (messagerie, Intranet ou Internet) et de les exploiter en cas d'incidents ou de manquements graves. »*

Exemple 2 :

> *« Une exploitation statistique des enregistrements est réalisée, sous forme anonyme, pour des motifs opérationnels. Elle consiste, notamment, à établir des statistiques relatives aux connexions et contacts réalisés.*
> *Néanmoins, l'entreprise peut procéder à des audits à caractère nominatif sur ces enregistrements informatiques, suite à un dysfonctionnement, une alerte de sécurité ou une*

présomption d'une utilisation non conforme des ressources informatiques, sous réserve du respect du secret de la correspondance privée et de la réglementation applicable.
En ce cas, les constatations matérielles ont pour but de relever les diverses circonstances qui éclaireront l'entreprise sur l'éventuelle réalisation d'un fait fautif et sur l'identité de son auteur. »

III.18. PROPRIETE INTELLECTUELLE

Des dispositions légales protègent le droit d'auteur et la propriété intellectuelle. Cette protection concerne notamment les logiciels, les contenus multimédias, les fichiers audio ou vidéo…

Afin d'éviter que les utilisateurs n'utilisent les ressources informatiques mises à leur disposition pour commettre des actes contraires au respect de la propriété intellectuelle, il convient de prévoir des mesures à ce propos dans la charte.

Notons que certaines dispositions applicables au titre de la sécurité du poste de travail peuvent également recouper les dispositions concernant la propriété intellectuelle, en ce qu'elles interdisent notamment l'installation de logiciels par des personnes non habilitées (ce qui vise également les logiciels dont l'utilisateur ne dispose pas de la licence d'utilisation).

« L'utilisateur ne recourra en aucune manière aux ressources informatiques, notamment les moyens de communication électronique, mises à sa disposition par l'employeur, pour lire, copier, stocker, ou transmettre, sans licence et à des fins privées ou commerciales, des contenus ou des logiciels protégés par le droit d'auteur et plus largement le droit de la propriété intellectuelle. »

III.19. COPIE DE LOGICIELS

Diverses propositions de rédaction sont possibles :

« Chaque utilisateur doit respecter des règles de bon usage et ne pas installer ou copier de logiciels même appartenant au domaine public. »

Il ne doit effectuer aucune copie de logiciels commerciaux même tombés dans le domaine public, pour quelque usage que ce soit.

« Conformément à la loi, il est rappelé que sauf autorisation expresse de l'entreprise, les logiciels, et les documents conçus ou réalisés par chaque utilisateur dans le cadre de son activité professionnelle sont la propriété de l'entreprise. »

III.20. EFFETS DU NON-RESPECT

Le salarié qui ne respectera pas les dispositions de la charte, s'expose à des sanctions disciplinaires, dans la mesure où la charte est annexée au règlement intérieur.

« *Cette infraction aux dispositions de la charte - dont le salarié a eu connaissance - étant susceptible de porter atteinte à la sécurité ainsi qu'au bon fonctionnement de l'entreprise, contrevient également au règlement intérieur de l'entreprise.*
Ce comportement expose le salarié, selon la nature et les circonstances de ses agissements, aux mesures disciplinaires prévues dans le règlement intérieur. »

ANNEXE 1 : SYNTHESE DU CADRE LEGAL ET REGLEMENTAIRE APPLICABLE AUX SYSTEMES D'INFORMATION

Cette énumération n'a pas vocation à être exhaustive mais à rappeler les grands textes et principes applicables qu'il convient de garder en mémoire lorsque l'on commence à rédiger une charte :

- Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (profondément modifiée par la loi du 6 août 2004) : cette loi vient encadrer les conditions dans lesquelles des données à caractère personnel peuvent être traitées.

- Loi du 29 juillet 1881 relative à la liberté de la presse, qui incrimine certains comportements commis au travers des médias de communication dans son chapitre IV (chapitre étendu à l'Internet par la Loi pour la Confiance dans l'Économie Numérique du 21 juin 2004).

- Art. 226-15 et 432-9 du Code pénal relatifs à l'interception et la destruction des correspondances privées.

- Loi du 10 janvier 1988 dite loi « Godfrain » : loi introduisant les articles 323-1 à 323-7 du Code pénal et prévoyant des sanctions contre les atteintes aux systèmes d'information. Ces articles ont été étendus et renforcés par la Loi pour la Confiance dans l'Économie Numérique du 21 juin 2004.

- Code de la propriété intellectuelle : ce code reprend les dispositions sur les droits d'auteur, le droit des marques ou encore le droit *sui generis* du producteur de bases de données.

- Article 226-13 du Code pénal relatif au secret professionnel et, pour les établissements financiers, article L. 511-33 du Code monétaire et financier relatif au secret bancaire.

- Pour les établissements financiers, règlement CRBF 97-02 modifié.

ANNEXE 2 : SYNTHESE DE LA JURISPRUDENCE APPLICABLE EN LA MATIERE

Là encore, cette énumération n'a pas vocation à être exhaustive mais plutôt à rappeler les principales décisions des tribunaux qu'il convient de garder en mémoire lorsque l'on commence à rédiger une charte.

Sur la responsabilité de l'employeur

- Arrêt de la Cour d'appel de Paris du 4 février 2004, *BNP Paribas*. Dans cette espèce, il avait été demandé à la société BNP Paribas d'identifier un de ses salariés auteur d'un message électronique litigieux, l'entreprise étant assimilée par le demandeur à un prestataire technique (fournisseur d'accès), ce qu'elle n'a pas contesté.
- Arrêt de la Cour d'appel d'Aix-en-Provence du 13 mars 2006, *Escota* (confirmation de la décision de première instance) : mise en cause de la responsabilité de l'employeur (Lucent) dans le cadre d'un site Internet au contenu illicite, créé par un de ses salariés (un mémo interne prévoyait un usage privé des ressources informatiques et n'interdisait pas spécifiquement ce type de d'acte).
- Arrêt de la Cour d'appel d'Aix-en-Provence du 17 janvier 2005 : Dans le cadre des faits précédemment cités, Lucent se retourne contre son salarié, auteur du site incriminé, à la suite de sa condamnation contre Escota en première instance.

Sur les notions de recevabilité de la preuve en droit social

- Arrêt de la Cour d'appel de Besançon du 9 sept 2003, *M. Rachid H. c/ SA Online Formapro* : absence d'information nécessaire sur le contrôle des logs vis-à-vis d'informaticiens. La cour estime qu'une telle information n'était pas nécessaire vis-à-vis d'un informaticien qui connaissait nécessairement l'existence de ce type de dispositif. Attention : cet arrêt d'espèce rendu par la Cour d'appel de Besançon paraît en totale contradiction avec la jurisprudence la plus récente de la Cour de Cassation exigeant non seulement l'information des salariés mais encore le respect des formalités auprès de la CNIL.
- Jugement du Conseil de prud'hommes de Nanterre du 16 juillet 1999 : la preuve apportée par IBM n'est pas admise en raison de son absence de traçabilité et d'imputabilité (disque dur conservé par IBM, présenté plusieurs mois après les faits).
- Arrêt de la Cour d'appel de Douai du 17 décembre 2004 : cette décision démontre que le placement sous scellé d'une preuve informatique ne signifie pas forcément sa recevabilité par les magistrats, en l'absence de traçabilité et d'imputabilité des actes.
- Arrêt de la Cour d'appel d'Aix-en-Provence du 17 décembre 2002 : décision mettant en avant la bonne traçabilité et imputabilité des actes au salarié (consultation de sites aux contenus éventuellement pédopornographiques).
- Arrêt de la Cour d'appel de Paris du 7 décembre 2004 : absence de la preuve d'imputabilité en l'absence de mot de passe personnel.
- Arrêt de la Cour d'appel de Rouen du 3 mai 2005 : absence d'imputabilité malgré des aveux.

Sur l'utilisation du contenu des messages personnels d'un salarié dans le cadre d'un licenciement

- Arrêt de la Cour de cassation du 2 octobre 2001, *Nikon*. « *L'employeur ne peut […] prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* ».

- Arrêt de la Cour de cassation confirmatif de l'arrêt *Nikon* du 12 octobre 2004. Cet arrêt reprend les principes de l'arrêt Nikon en visant directement la messagerie électronique.
- Arrêt de la Cour d'appel de Douai du 30 septembre 2003, *Mme Clémentine L. c/ SA Interactive Speech*. Cet arrêt est une autre application de la jurisprudence Nikon aux contenus des emails personnels.
- Arrêt de la Cour d'appel de Paris du 17 décembre 2001 : interception de correspondance dans une école d'ingénieurs de la Ville de Paris (consultation de la messagerie d'un étudiant accusé de fraudes par un administrateur système).
- Arrêt de la Cour d'appel de Chambéry du 6 novembre 2003, *Mme Anne O. c/ CGEA Annecy* : les messages professionnels ne peuvent bénéficier de la protection accordée à la correspondance privée.
- Arrêt de la Cour d'appel de Paris du 12 mai 2005 : les contenus pornographiques ne sont pas protégés par le secret des correspondances.

Sur l'utilisation du contenu des fichiers personnels d'un salarié dans le cadre d'un licenciement

- Arrêt de la Cour d'appel de Bordeaux du 10 juin 2002 : la preuve d'un licenciement peut valablement être fondée à partir du recueil de fichiers personnels du salarié sur une disquette appartenant à l'employeur.
- Arrêt de la Cour de cassation du 17 mai 2005, *Cathnet* : la découverte de photos pornographiques sous format papier sur un bureau est insuffisante à justifier une fouille exhaustive d'un ordinateur. Une telle recherche doit normalement être effectuée en présence du salarié ou celui-ci dûment appelé, sauf dans le cas où les circonstances l'exigent (existence d'un risque particulier).

Sur l'obligation ou non de prévoir un usage privé des ressources informatiques :

- Arrêt de la Cour d'appel de Versailles du 18 mars 2003 : cet arrêt est en faveur de la reconnaissance d'un usage privé mais a été rendu dans une circonstance particulière où l'employeur remettait un ordinateur portable professionnel hors des heures de travail avec interdiction d'en faire un usage privé… mais pas d'interdiction non plus d'en faire un usage professionnel en-dehors des heures de travail.
- Arrêt de la Cour d'appel de Douai du 28 février 2005 : cet arrêt précise qu'il apparaît possible d'interdire strictement tout usage privé des ressources informatiques par la voie du règlement intérieur, même si cette question n'était pas au centre du litige tranché.

Sur le principe de labellisation des messages :

- Jugement du Conseil de prud'hommes de Nanterre du 15 septembre 2005 reconnaissant la validité de la procédure prévue dans un règlement intérieur encadrant la correspondance privée (labellisation des messages).

Sur la présomption de caractère professionnel des fichiers créés par le salarié

- Arrêt de la Cour de cassation du 18 octobre 2006, *Techni-Soft* : les fichiers créés par le salarié à l'aide de l'outil informatique mis à sa disposition sont présumés avoir, sans identification particulière, un caractère professionnel. L'employeur peut y avoir accès sans formalisme ou autorisation spécifiques. Dès lors, le chiffrement par le salarié de ces données rendant leur accès impossible à l'employeur est constitutif d'une faute justifiant, en l'espèce, le licenciement.

Sur les limitations reconnues à l'usage des ressources informatiques :

- Arrêt de la Cour de cassation du 19 mai 2004, *Nortel* : le détournement des ressources informatiques mises à disposition par l'employeur afin de gérer un site échangiste en entreprise peut être constitutif d'abus de confiance.
- Arrêt de la Cour de cassation du 25 janvier 2005, *Clear Channel* : interdiction d'envoi a priori de courriers électroniques syndicaux dans l'entreprise ou à des salariés de l'entreprise sans accord préalable avec l'employeur.
- Arrêt de la Cour de cassation du 2 juin 2004 : confirmation d'un licenciement effectué en raison de l'envoi d'un courriel antisémite dans une entreprise (la Cour indiquant qu'un tel acte était susceptible d'entraîner la responsabilité éventuelle de l'employeur).

ANNEXE 3 : LISTE DES MEMBRES DU GROUPE DE TRAVAIL

Ce document a été rédigé par un groupe de travail composé de :

Prénom	Nom	Etablissement
François	COUPEZ	SOCIETE GENERALE
Christine	HUYNH QUAN SUU	AGENCE FRANCAISE DE DEVELOPPEMENT
Damien	JULLEMIER	LCL
Sabine	MARCELLIN	LA BANQUE POSTALE

Il n'aurait pu être réalisé sans l'aide des personnes ayant contribué à son élaboration ou à sa relecture :

Prénom	Nom	Etablissement
Joël	FERRY	Représentant de la GENDARMERIE NATIONALE AU MINISTERE DE LA JUSTICE
Wilfrid	GHIDALIA	FORUM DES COMPETENCES
Xavier	LEMARTELEUR	SOCIETE GENERALE
Christian	NGUYEN DUY MAT	BANQUE FINAMA
Georges	TROUBLAIEWITCH	BANQUE FINAMA

Ce document a pour objet de fournir des clefs utiles à prendre en compte lors de la rédaction et de la mise en place d'une charte d'utilisation des ressources informatiques et de communication électronique. Il est illustré d'exemples concrets et réels. Cependant, chaque entreprise doit tenir compte de sa spécificité lors de l'élaboration de sa charte. Ce document n'a donc pas vocation à se substituer aux conseils d'un avocat ou d'un juriste d'entreprise.

BIBLIOGRAPHIE

- CIGREF, « *Déontologie des usages des systèmes d'information. Principes fondamentaux* » - janvier 2006

- Commission Nationale de l'Informatique et des Libertés (CNIL), « *Guide pratique pour les employeurs* » - octobre 2005

- Association Française de l'Audit et du Conseil Informatique (AFAI), « *Charte d'utilisation des systèmes de base de connaissance* » - mai 2005

- Commission Nationale de l'Informatique et des Libertés (CNIL), rapport sur la « *La cybersurveillance sur les lieux de travail* » - mars 2004

- MEDEF, Vade-mecum « *L'utilisation des nouvelles technologies dans l'entreprise* » - février 2003

- Forum des droits sur l'internet, rapport sur les « *Relations de travail et l'internet* » - septembre 2002