DDN/RSSI

Guide juridique sur l'usage du système d'information

SOMMAIRE

ARTICLE I. PRÉAMBULE

Le présent guide juridique de l'utilisateur s'inscrit dans le cadre de la politique de sécurité de l'université d'Angers (dénommé ci-après « établissement »).

Le guide est pris en application des règles édictées dans la charte des systèmes d'information, dans le prolongement de laquelle il s'inscrit ; il la complète.

Afin de faciliter la bonne compréhension de cette charte, l'établissement a rédigé le présent document intitulé « guide juridique de l'utilisateur », dont l'objectif est de présenter les règles de droit qui ont présidé à la rédaction de cette charte, ainsi que les risques liés au non respect de ces règles.

Il est donc recommandé à chaque utilisateur de procéder à une lecture attentive de ce guide.

Ce guide, bien qu'il s'efforce d'être exhaustif, ne saurait cependant être considéré comme limitatif. En effet, compte tenu de la multiplicité des règles relatives au bon usage des ressources informatiques et de communication électronique, il appartient avant tout à l'utilisateur d'adopter en toutes circonstances un comportement prudent et avisé.

La complexité, tant sur le plan juridique que technique, des règles en question explique que l'établissement ait pris l'initiative de diffuser des documents explicatifs ayant pour objectif d'exposer sur un plan pratique les principes de mise en œuvre des règles définis dans la charte.

La charte des systèmes d'information doit être interprétée en fonction du présent guide juridique et du livret technique.
En application de l'article L.1321-1 du Code du travail :

- Le règlement intérieur est un document écrit par lequel l'employeur fixe exclusivement :

  - Les mesures d'application de la réglementation en matière de santé et de sécurité dans l'entreprise ou l'établissement, notamment les instructions prévues à l'article L. 4122-1 ; (…)

- Les règles générales et permanentes relatives à la discipline, notamment la nature et l'échelle des sanctions que peut prendre l'employeur ».

- L'article L. 1321-5 dispose notamment que « les notes de service ou tout autre document comportant des obligations générales et permanentes dans les matières mentionnées aux articles L.1321-1 et L. 1321-2 sont, lorsqu'il existe un règlement intérieur, considérées comme des adjonctions à celui-ci. Ils sont, en toute hypothèse, soumis aux dispositions du présent titre ».

- En ce qu'elle définit des « obligations générales et permanentes » aux fins de garantir notamment la sécurité des moyens informatiques et de communication électronique de l'établissement, obligations sanctionnées s'il y a lieu sur le plan disciplinaire, la charte est une annexe au règlement intérieur.

- La charte a été portée à la connaissance des utilisateurs et entrera en vigueur à compter de [.] et du respect de la procédure d'établissement du règlement intérieur ».

ARTICLE II. RESPECT DES LOIS ET REGLEMENTS

L'établissement met à la disposition des utilisateurs, dans le cadre de leur activité professionnelle, des ressources informatiques et de communication électronique, dont l'usage est source de responsabilité.

Les faits commis sont en effet susceptibles d'entraîner la mise en cause de la responsabilité civile[1] ou pénale[2] tant de l'établissement que des utilisateurs.

Il est, en revanche, important de préciser que le statut d'employé (public ou privé)[3] ne protège en aucune manière l'utilisateur d'une mise en cause de sa responsabilité civile ou pénale en cas d'utilisation illicite de ces moyens.

Il existe donc une obligation pour l'établissement de définir les règles d'utilisation de ses ressources informatiques et de communication électronique aux fins de la préserver, ainsi que les utilisateurs, de toute mise en cause de leur responsabilité respective.

Il s'agit précisément de l'objet de la charte dont les fondements juridiques sont exposés dans le présent guide juridique.

L'utilisation desdits moyens doit ainsi répondre à un référentiel qui inclut notamment :

- la législation et la réglementation en vigueur ;
- la jurisprudence ;
- les recommandations d'organismes ou d'autorités compétents ;
- les meilleures pratiques du domaine.

Sans que cette liste ait un caractère exhaustif, les réglementations applicables sont relatives :

- à la protection des systèmes d'information, et notamment à la fraude informatique, qu'il s'agisse de l'intrusion dans un système d'information ou de l'altération des informations qu'il contient, étant précisé que ces actes sont passibles de sanctions pénales ;

[1] Article 1384 du Code civil : « On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde. Toutefois, celui qui détient, à un titre quelconque, tout ou partie de l'immeuble ou des biens mobiliers dans lesquels un incendie a pris naissance ne sera responsable, vis-à-vis des tiers, des dommages causés par cet incendie que s'il est prouvé qu'il doit être attribué à sa faute ou à la faute des personnes dont il est responsable. Cette disposition ne s'applique pas aux rapports entre propriétaires et locataires, qui demeurent régis par les articles 1733 et 1734 du code civil. Le père et la mère, en tant qu'ils exercent l'autorité parentale, sont solidairement responsables du dommage causé par leurs enfants mineurs habitant avec eux. Les maîtres et les commettants, du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés ; Les instituteurs et les artisans, du dommage causé par leurs élèves et apprentis pendant le temps qu'ils sont sous leur surveillance. La responsabilité ci-dessus a lieu, à moins que les père et mère et les artisans ne prouvent qu'ils n'ont pu empêcher le fait qui donne lieu à cette responsabilité. En ce qui concerne les instituteurs, les fautes, imprudences ou négligences invoquées contre eux comme ayant causé le fait dommageable, devront être prouvées, conformément au droit commun, par le demandeur, à l'instance. »

[2] L'article L. 121-2 du Code pénal dispose : « Les personnes morales, à l'exclusion de l'État, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7, des infractions commises, pour leur compte, par leurs organes ou représentants. (…) La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits, sous réserve des dispositions du quatrième alinéa de l'article 121-3. »

[3] Cette mise en garde est également valable pour les stagiaires, intérimaires, intervenants extérieurs tels que les consultants, prestataires ou auditeurs.

- à la propriété intellectuelle, et notamment aux droits d'auteur qu'il s'agisse de créations multimédia, de logiciels, de textes, de photos, d'images ou d'œuvre de toute autre nature ;

- aux libertés individuelles, et notamment aux dispositions légales en matière de traitements de données à caractère personnel ;

- au respect des règles d'ordre public en matière de contenu des informations qui seraient susceptibles d'être mises en ligne sur le réseau, telles que des informations à caractère pornographique ou portant atteinte à l'intégrité ou à la sensibilité d'un autre utilisateur par accès à des messages, images ou textes provocants ;

Ces dernières années, les plus hautes juridictions nationales ont rendu de nombreuses décisions sur l'utilisation des ressources informatiques et de communication électroniques à des fins personnelles[4], ainsi que sur la preuve de la faute de l'employé par des procédés informatiques.

A plusieurs reprises, la Cour de cassation notamment s'est prononcée sur la problématique de l'usage professionnel et l'usage non professionnel de ces moyens.

la Commission nationale de l'informatique et des libertés (Cnil)[5]œuvre également à la réflexion sur, d'une manière générale, la problématique de la cyber surveillance dans le domaine du travail.

La Cnil de son côté a publié en 2010 un guide, présenté sous formes de fiches pratiques sur des thématiques clés, à destination des employeurs et des salariés[6]. Ces fiches traitent des données à caractère personnel dans l'univers spécifique des dispositifs de contrôle des employés liés aux nouvelles technologies. L'objectif est, d'une part, de répondre à un souci de transparence et de confiance à l'égard des employés, et d'autre part, de garantir la sécurité juridique pour les entreprises, en leur qualité de responsables de traitement.

Le 12 octobre 2009, la Cnil a publié sur son site web « 10 conseils pour sécuriser votre système d'information ».[7]

Sans entrer dans le détail de ces 10 conseils, il convient de relever que les conseils n°9 et 10, respectivement « anticiper et formaliser une politique de sécurité du système d'information » et « sensibiliser les utilisateurs aux risques informatiques et à la loi informatique et libertés », suggèrent à l'entreprise d'aller au-delà de la simple rédaction d'une charte et de mettre en place une véritable gouvernance de la sécurité, les utilisateurs du système d'information devant être particulièrement sensibilisés aux risques informatiques.

[4] Un arrêt a marqué le développement du contentieux en la matière en ce qu'il est considéré comme l'arrêt fondateur du concept de « vie privée résiduelle », soit : Cass. soc.2-10-2001 n° 99-42942 dit arrêt « Nikon ».
[5] Le site internet de la Cnil est accessible à l'adresse suivante : www.cnil.fr.
[6] Guide pour les employeurs et les salariés, Cnil, 2008.
[7] 10 conseils pour sécuriser votre système d'information, Cnil, 12-10-2009.

ARTICLE III. REGLES D'UTILISATION DU SYSTEME D'INFORMATION

SECTION III.1 CONDITIONS D'ACCÈS ET D'IDENTIFICATION

L'établissement définit :

- les conditions d'accès aux moyens informatiques et de communication électronique qu'il met à disposition ;
- les conditions de suspension et de retrait de cet accès dont il en informera l'utilisateur concerné dans la mesure du possible » ;

L'utilisateur se voit attribuer un identifiant ayant un caractère confidentiel. Pour des raisons de protection, de sécurité ou de continuité du service il pourra être demandé à l'utilisateur de communiquer son identifiant ».

La jurisprudence est relativement dense en la matière. Il peut ainsi être rappelé que :

- la chambre sociale de la Cour de cassation a considéré que dans l'hypothèse notamment de l'absence prolongée pour maladie ou congé sabbatique, il pourra être demandé à l'utilisateur de communiquer son identifiant, dont la rétention constituerait un acte d'insubordination justifiant son licenciement pour faute grave ;

- une cour d'appel a ainsi jugé que repose sur une cause réelle et sérieuse le licenciement prononcé à l'encontre de la salariée qui « En refusant de répondre favorablement à une demande d'information isolée alors que, s'agissant d'un numéro de code d'accès informatique, elle était en mesure d'y répondre sans investigation préalable et savait pertinemment que son refus mettait en difficulté la personne qui la remplaçait et son employeur, la salariée a manqué aux obligations de bonne foi et de loyauté qui lui incombait et n'étaient pas supprimées pendant la suspension de son contrat de travail » ;

- dans un arrêt du 18 mars 2003 , la Cour de cassation a retenu la notion de la continuité du service pour sanctionner la non-communication des codes d'accès informatique en considérant que « Si le salarié n'est pas tenu de poursuivre une collaboration avec l'employeur durant la suspension de l'exécution du contrat de travail provoquée par la maladie ou l'accident, l'obligation de loyauté subsiste durant cette période et le salarié n'est pas dispensé de communiquer à l'employeur, qui en fait la demande, les informations qui sont détenues par lui et qui sont nécessaires à la poursuite de l'activité de l'entreprise ; d'où il suit qu'en statuant comme elle l'a fait, sans rechercher si l'employeur avait effectivement la possibilité, sans recourir à la salariée, d'avoir communication du mot de passe informatique et si de ce fait, comme le soutenait l'employeur en demandant la confirmation du jugement, la salariée n'avait pas eu une volonté de bloquer le fonctionnement de l'entreprise, la cour d'appel a violé les textes susvisés ».

L'article 226-4-1 du Code pénal incrimine le fait d'usurper l'identité d'un tiers ou de faire usage de données permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, y compris lorsque ce délit est commis sur un réseau de communication au public en ligne. Les peines peuvent atteindre un an d'emprisonnement et 15000 euros d'amende.

SECTION III.2 USAGE DES RESSOURCES INFORMATIQUES ET DE COMMUNICATION ÉLECTRONIQUE

La problématique majeure est la distinction entre l'usage professionnel et l'usage non professionnel des ressources informatiques et de communication électronique mis à disposition des utilisateurs par l'établissement en vue de l'accomplissement des tâches qui leurs sont confiées.

Par deux décisions du 18 octobre 2006[8], la Cour de cassation a précisé que les dossiers et fichiers créés par un salarié, grâce aux outils informatiques et de communication électronique mis à sa disposition par son employeur pour l'exécution de son travail, sont présumés, sauf si le salarié les identifie comme personnels, avoir un caractère professionnel. Il en résulte que l'employeur peut y avoir accès hors sa présence.

De fait, si la Cour de cassation légitime, d'un côté, le droit d'accès de l'employeur aux fichiers et aux messages électroniques reçus et émis par ses salariés, elle légitime, de l'autre côté, l'utilisation de ces mêmes outils à des fins personnelles, au nom du principe communément dénommé « vie privée résiduelle »[9].
La Cour de cassation concilie les intérêts de l'employeur, pouvant mettre en place des dispositifs de contrôle de l'activité de ses salariés afin de réduire les risques d'engagement de sa responsabilité, et les droits fondamentaux des salariés tenant entre autre au respect de leur vie privée, principe protégé tant au niveau national[10] qu'au niveau européen[11].
Il convient ici de relever que le droit au respect de la vie privée, en ce compris le respect des correspondances privées, s'applique non seulement dans la relation entre l'établissement et les utilisateurs, mais également dans les relations entre utilisateurs sous peine d'engager leur responsabilité civile et pénale, et de subir des sanctions disciplinaires.

Il est donc indispensable pour l'établissement de bien déterminer la frontière entre l'usage professionnel et l'usage personnel des outils qu'elles mettent à disposition.

Dans le cadre d'un usage non professionnel des systèmes d'information, l'utilisateur est tenu, s'il souhaite émettre ou recevoir des courriers électroniques ou utiliser un répertoire informatique à titre privé, de mentionner dans l'objet le terme « PRIVE – PERSONNEL.

Il a, en effet, été considéré par la chambre sociale de la Cour de cassation, dans un arrêt du 21 octobre 2009, que tous les répertoires informatiques et échanges électroniques ne portant pas la mention « PRIVE - PERSONNEL » sont considérés comme de nature professionnelle[12].

---

[8] Cass. soc. 18-10-2006 n°04-48025 : « 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 de sorte que l'employeur peut y avoir accès hors sa présence » ; Cass. soc. 18-10-2006 n°04-47400 : « Les documents détenus par le salarié dans le bureau

[9]de l'entreprise mis à sa disposition sont, sauf lorsqu'il les identifie comme étant personnels, présumé avoir un caractère professionnel, e sorte que l'employeur peut y avoir accès hors de sa présence ».

Cass. soc.2-10-2001 n° 99-42942 dit arrêt « Nikon »: « (…) Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale 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 ».

[10] Soit notamment le Code civil (art.9 et 1384), le Code pénal (art. 226-15 et 432-9), le Code du travail (art.L. 2323-13) et la loi dite « Informatiques et libertés ».

[11] Convention de sauvegarde des droits de l'Homme et des libertés fondamentales (art. 8).

[12] Cass. soc. 21-10-2009 n°07-4387.

La chambre sociale de la Cour de cassation a par ailleurs précisé que si l'employeur peut consulter les fichiers qui n'ont pas été identifiés comme personnels par l'employé, il ne peut les utiliser à son encontre dans une procédure judiciaire s'ils s'avèrent que les informations qu'il contient relève de la vie privée[13].

En pratique, deux grandes tendances coexistent:

- Certains acteurs ont défini une règle de nommage des fichiers et messages électroniques personnels, en imposant à leurs utilisateurs d'utiliser un terme prédéfini pour qualifier ces éléments de « personnel » (le terme le plus répandu étant « privé ») ;

- d'autres ont fait le choix de considérer que l'adresse électronique fournie par elles est exclusivement réservée à un usage professionnel, tout en permettant et en facilitant l'utilisation de services internet gratuits de type webmail[14].

Pour des raisons de sécurité, l'établissement a opté pour une définition des règles de nommage.

Il n'en demeure pas moins que l'usage des ressources informatiques et de communication électronique à des fins personnelles, quelles qu'en soient les modalités pratiques, doit demeurer exceptionnel.

Au même titre qu'un document papier, un document électronique doit être conservé et archivé puisqu'il peut constituer une preuve.

Section III.3 Gestion des absences et des départs

En cas d'absence, l'établissement se réserve le droit de :

- accéder aux éléments présents au sein des moyens informatiques et de communication électronique mises à disposition de l'utilisateur concerné, en ce qu'ils sont présumés professionnels ;

- accéder, sous certaines conditions, aux fichiers, répertoires et messages informatiques clairement dénommés « PRIVE ».

En cas de départ, l'utilisateur perd tout droit d'accès au système d'information et de communication sauf décision contraire de l'autorité hiérarchique de l'utilisateur.

Section III.4 Plan de continuité d'activité

En présence de toute situation susceptible de porter atteinte à la continuité du service, l'établissement peut prendre toute mesure adéquate.

Les utilisateurs doivent apporter leur concours à cette mise en place.

Section III.5 Mobilité et matériels mis à disposition par l'établissement

En cas de prêt par l'établissement d'un équipement nomade (ordinateur portable, cellulaire, tablette…), l'utilisateur est responsable du matériel qui lui a été confié.

Dans certains pays étrangers les contrôles douaniers permettent la saisie temporaire et le contrôle du contenu du matériel informatique.

[13] Cass. soc. 7-7-2011 n°10-25706.

[14] Le webmail est une interface web rendant possible l'émission, la consultation et la manipulation de courriers électroniques directement sur le web depuis un navigateur

ARTICLE IV. LA PROTECTION DES DONNEES À CARACTÈRE PERSONNEL

SECTION IV.1 PRINCIPES

Les données à caractère personnel font l'objet d'une protection légale particulière dont la violation expose son auteur à des sanctions pénales.

Les textes applicables en la matière sont les suivants :

- la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 ;

- la convention n°108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

- la directive n°95/46 du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

- la directive n°2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication, et modifiant la directive 2002/58/CE ;

- la directive n°2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

Ces règles s'appliquent à l'ensemble des systèmes de traitement de l'information dès lors que cette information permet d'identifier un ou plusieurs individus.

La loi du 6 janvier 1978 a créé un dispositif juridique pour encadrer la mise en œuvre des « traitements automatisés de données à caractère personnel » et ouvrir aux individus un droit d'accès et de rectification sur les données les concernant détenues et gérées par des tiers.

Cette loi impose de procéder à une demande préalable (déclaration, autorisation ou avis) à la mise en œuvre d'un tel traitement automatisé auprès de la Commission Nationale de l'Informatique et des libertés (Cnil)

Est considérée comme donnée à caractère personnel toute information permettant l'identification directe ou indirecte d'un individu, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Ainsi, constituent des données à caractère personnel, sans que cette liste soit exhaustive[15] :

- le nom,
- les numéros de téléphone,
- les numéros d'immatriculation de véhicule,
- les numéros ou codes d'identification d'une personne,
- les numéros de compte bancaire,
- le numéro de sécurité sociale ou le numéro d'identification au répertoire (NIR),
- l'adresse postale, l'adresse e-mail,
- la photographie,
- l'adresse IP.

Est considéré comme traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé.

La loi du 6 janvier 1978 a créé un dispositif juridique, pour encadrer la collecte et la mise en œuvre des traitements des données à caractère personnel, en vertu duquel :

- d'une part, il est interdit, sauf exceptions limitativement énumérées, de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci ;

- d'autre part, toute personne auprès de laquelle sont collectées (oralement ou par écrit) des informations mises en œuvre dans un système automatisé de traitement doit être informée :

  - de l'identité du responsable du traitement ;

  - de la finalité du traitement ;

  - du caractère obligatoire ou facultatif des réponses ;

  - des conséquences d'un défaut de réponse ;

  - des destinataires des informations ;

  - de l'existence d'un droit d'interrogation, d'accès, de rectification, d'opposition pour motifs légitimes, sur les données à caractère personnel les concernant détenues et gérées par des tiers ;

  - le cas échéant, des flux transfontières de données à caractère personnel.

[15] L'ajout de ces exemples de données à caractère personnel permet de donner aux personnels de l'établissement des exemples concrets de données à caractère personnel et rend ces dispositions plus intelligibles.

Le responsable de traitement est la personne qui détermine les finalités et les moyens du traitement. A ce titre, il est tenu de procéder à une collecte loyale et licite des données à caractère personnel, étant précisé que les finalités de la collecte doivent être déterminées, explicites et légitimes.

L'article 34 de la loi n° 78-17 du 6 janvier 1978 dispose que « le responsable d'un traitement doit prendre toutes les précautions utiles afin de préserver la sécurité des données, et notamment d'empêcher qu'elles ne soient déformées, endommagées ou que des tiers non autorisés y aient accès ».
Le responsable de traitement est tenu de :

- corriger les données à caractère personne inexactes ou incomplètes au regard des finalités pour lesquelles elles ont été collectées ;
- conserver les données à caractère personne sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ;
- assurer la sécurité et la confidentialité des données à caractère personnel, y compris dans le cas où le traitement serait sous-traité à un tiers, ce dernier devant présenter des garanties suffisantes formalisées dans un contrat écrit ;
- informer, la personne dont les données à caractère personnel sont collectées, oralement ou par écrit, comme indiqué ci- dessus »[16].

La personne concernée est la personne physique à laquelle se rapportent les données qui font l'objet du traitement.

Cette personne bénéficie de :
- un droit d'opposition, qui lui permet de s'opposer pour des motifs légitimes que ses données fassent l'objet d'un traitement ;
- un droit d'accès, qui lui permet d'obtenir la communication d'un certain nombre d'informations relatives aux données traitées ;
- un droit de modification ou de suppression de ses données.

SECTION IV.2 SANCTIONS

La non application de la loi Informatique et Libertés peut être sanctionnée pénalement.

Les infractions les moins graves (défaut d'information, défaut de réponse à une demande de rectification) sont sanctionnées par des amendes de 5° classe, mais la plupart des violations de la loi Informatique et Libertés sont lourdement sanctionnées d'une peine maximum de 5 ans d'emprisonnement et de 300.000 euros d'amende. Il en est par exemple ainsi du non respect y compris par négligence, des formalités préalables, du non respect de l'obligation de sécurité, ou encore du non respect de la durée de conservation des données.

[16] L'article 35 de la loi n°78-17 du 6 janvier 1978 modifiée énonce en effet que « les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.

Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi.

Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement ».

Constitue une infraction le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les règles posées par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée.

ARTICLE V. LA PROTECTION DES DROITS DE PROPRIÉTÉ INTELLECTUELLE

SECTION V.1 LES RÈGLES DE PROTECTION DU DROIT D'AUTEUR

En vertu des règles du Code de la propriété intellectuelle, l'auteur d'une œuvre de l'esprit jouit sur cette œuvre du seul fait de sa création « d'un droit de propriété incorporel et exclusif opposable à tous ».

Cette disposition s'applique à toutes les œuvres de l'esprit quel qu'en soit le genre, la forme d'expression, le mérite ou la destination.

Sont notamment considérées comme des œuvres de l'esprit, au sens du Code de la propriété intellectuelle et en particulier de l'article L.112-2, les œuvres suivantes :

- *les livres, brochures et autres écrits littéraires, artistiques et scientifiques ;*
- *les conférences, allocutions et autres œuvres de même nature ;*
- *les œuvres dramatiques ou dramatico-musicales ;*
- *les œuvres chorégraphiques, ... ;*
- *les œuvres musicales avec ou sans paroles ;*
- *les œuvres cinématographiques et autres œuvres consistant dans des séquences animées d'images sonorisées ou non, dénommées ensemble œuvres audiovisuelles;*
- *les œuvres de dessins, de peintures, d'architectures, de sculptures, de gravures, de lithographies ;*
- *les œuvres graphiques et typographiques ;*
- *les œuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie ;*
- *les œuvres d'art appliqué ;*
- *les illustrations, les cartes géographiques ;*
- *les logiciels, y compris le matériel de conception préparatoire...* ».

Les actes de reproduction et de représentation des œuvres protégées en tout ou partie, par tout moyen et sous toute forme sont ainsi soumis à l'autorisation du/ou des titulaire(s) des droits sur les œuvres.

L'utilisation de ces œuvres suppose donc une acceptation préalable du /ou des titulaire(s) des droits.

L'utilisateur est donc informé qu'à défaut d'une autorisation expresse du/ou des titulaire(s) respectant les dispositions du Code de la propriété intellectuelle, il lui est interdit d'utiliser une telle œuvre.

A défaut, sa responsabilité civile et/ou pénale peut être engagée.
En 2009, un nouveau dispositif a été adopté en deux temps :

- loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, dite « Loi Hadopi 1 » ;

- loi n°2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet, dite « Loi Hadopi 2 ».

Ces lois ont été adoptées pour tirer les conséquences des difficultés d'application de la loi DADVSI, loi relative au droit d'auteur et aux droits voisins dans la société de l'information, qui avait privilégié le mécanisme des DRM.
Cette nouvelle réglementation repose sur deux éléments importants, qui sont d'une part, de nouvelles dispositions juridiques, avec de nouvelles sanctions, et d'autre part une nouvelle autorité chargée du contrôle de l'application de la loi, l'Hadopi (Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet).

L'Hadopi a un pouvoir relativement étendu sur la diffusion et la protection des œuvres sur Internet. Sa mission est préventive, mais elle intervient également dans le cadre d'un processus répressif, sans toutefois pouvoir prendre la décision finale, qui appartient au juge judiciaire.

Le nouveau droit comprend deux axes :

- Un renforcement des peines à l'encontre de l'auteur d'un téléchargement illicite, la loi prévoyant des peines complémentaires aux peines d'amende et d'emprisonnement encourues, consistant en la suspension de l'accès à Internet pour une durée maximale d'un an.

- La responsabilité du titulaire de l'accès à Internet est également susceptible d'être engagée (en l'espèce l'établissement…). La réglementation impose à l'abonné de veiller à ce que l'accès à Internet ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires lorsqu'elle est requise.

  Dans certaines conditions, si l'abonné ne met pas en œuvre un moyen de sécurisation de son accès à Internet, malgré les recommandations reçues de l'Hadopi, celui-ci pourrait se voir condamner à une peine complémentaire de suspension d'accès à Internet pour une durée maximale d'un mois.

  Ces dispositions légitiment les mesures prises pour empêcher que les moyens de communication électronique ne soient utilisés pour réaliser des téléchargements illicites.
  Elles légitiment également le fait que ces outils permettent l'analyse des conditions dans lesquelles les internautes téléchargent des contenus et il est strictement interdit pour l'utilisateur de supprimer ou altérer le fonctionnement des mesures techniques mises en œuvre pour empêcher le téléchargement, de même qu'il est interdit de modifier les données relatives à l'usage de ces outils.

  Par ailleurs, au sein de l'établissement, toute personne qui recevrait une information ou un courrier électronique provenant d'un fournisseur d'accès à Internet ou de l'Hadopi, devrait en informer sa hiérarchie afin que les mesures appropriées soient prises.

SECTION V.2 LES RÈGLES DE PROTECTION DES LOGICIELS

Il résulte des articles L.112-1 et L.112-12, 13° du Code de la propriété intellectuelle que les logiciels sont protégés par le droit d'auteur en tant qu'œuvres de l'esprit.

Toute reproduction, adaptation et/ou distribution du logiciel n'est autorisée que sous réserve du consentement du titulaire des droits sur ledit logiciel.

L'étendue et les caractéristiques des droits conférés sont définies en général par des contrats de licence d'utilisation qui précisent les modalités selon lesquelles est autorisée l'utilisation des logiciels visés.

L'utilisation du logiciel, même à des fins d'essais, de démonstration de courte durée ou à des fins pédagogiques et à défaut d'autorisation expresse et écrite du titulaire des droits est en principe interdite.

L'utilisateur d'un logiciel s'expose à des sanctions civiles et pénales prévues et réprimées par le Code de la propriété intellectuelle lorsqu'il utilise un logiciel sans autorisation.

Afin de prévenir les risques liés à la contrefaçon de logiciel, une vigilance particulière des utilisateurs comme de leur autorité hiérarchique est indispensable.

L'utilisateur ne peut par exemple enregistrer ou télécharger un programme auquel il a eu accès dans le cadre de ses fonctions au sein de l'établissement afin de l'enregistrer sur son propre poste pour toute autre utilisation hors du cadre de ses fonctions et/ou hors de l'établissement sans autorisation et/ou habilitation à cet effet.

De la même manière, l'utilisateur ne peut enregistrer ou télécharger sur des équipements de l'établissement des logiciels sur lesquels des droits lui auraient été concédés à titre personnel et dont l'utilisation à des fins professionnelles au sein de l'établissement ne rentrerait pas dans le cadre de l'étendue des droits conférés sur l'œuvre en question.

Est un délit de contrefaçon puni par le Code de la propriété intellectuelle, (article L.335-3 du Code de la propriété intellectuelle) toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur ainsi que la violation de l'un des droits de l'auteur d'un logiciel.

Les logiciels dits « libres » comme par exemple les logiciels « shareware » sont en libre essai mais non libres de droits.

Il existe des licences associées notamment la licence « GPL » qui est une licence qui contient des droits et obligations à la charge de l'auteur et de l'utilisateur.

Les utilisateurs sont informés que de tels actes exposent également l'établissement à des risques importants, notamment en termes de sécurité informatique.

SECTION V.3 LES RÈGLES DE PROTECTION DES DONNÉES ET DES BASES DE DONNÉES

De la même façon, les données telles que les textes et, dès lors que ceux-ci présentent une certaine originalité, les images et les sons, sont protégés par le droit d'auteur.

L'autorisation écrite du titulaire des droits est ainsi nécessaire pour leur utilisation.

Le non-respect des dispositions relatives à la protection des droits de l'auteur sur ces données est constitutif de contrefaçon et il est donc civilement et/ou pénalement sanctionnable.

D'une manière générale, la difficulté à connaître précisément l'origine des données transmises et donc les droits y afférents, en particulier avec le développement des moyens d'échanges d'informations en réseau ouvert comme Internet, oblige les utilisateurs à la plus grande prudence.

On entend par bases de données un recueil d'œuvres de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou par tout autre moyen.

Les bases de données sont protégées par le Code de la propriété intellectuelle indépendamment de la protection dont peuvent bénéficier les données au titre du droit d'auteur contenu dans ladite base.

Les bases de données qui, par le choix ou les dispositions des matières, constituent des créations intellectuelles, bénéficient des dispositions du Code de la propriété intellectuelle.

L'utilisateur est susceptible de se rendre coupable du délit de contrefaçon lorsqu'il procède sans autorisation ou habilitation :

- à toute extraction par transfert permanent ou temporaire de la totalité ou en partie qualitativement ou quantitativement substantielle, du contenu de cette base de données sur un autre support, par tout moyen et sous toute forme que ce soit ;

- à la réutilisation ou à la mise à disposition de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base quelle que soit sa forme.

A ce titre, un utilisateur des bases de données de l'établissement ne saurait s'autoriser à utiliser à des fins privées par exemple un fichier d'adresses, dont l'établissement est propriétaire, et ne saurait le télécharger ou en faire toute utilisation contraire au Code de la propriété intellectuelle.

ARTICLE VI. LA PROTECTION DES MARQUES

Le Code de la propriété intellectuelle protège « toute marque de fabrique, de commerce ou de service servant à distinguer les produits ou services d'une personne physique ou morale » (article L.711-1)

Peuvent être définis et utilisés à titre de marque, tous signes nominaux, figuratifs ou sonores, tels que les mots, assemblage de mots, nom patronymique, nom géographique, pseudonyme, lettre, chiffre, sigle, emblème, photographie, dessin, empreinte, logo ou la combinaison de certains d'entre eux.

Ces droits et leur protection sur une marque, confèrent à son titulaire par un enregistrement, un droit de propriété sur cette marque.
L'utilisateur ne peut, sauf autorisation du propriétaire, reproduire, utiliser ou apposer une marque, ainsi qu'utiliser une marque protégée, supprimer ou modifier une marque régulièrement déposée.

Les utilisateurs s'interdisent donc, sauf autorisation expresse du propriétaire, toute reproduction ou usage ou apposition d'une marque ainsi que l'usage d'une marque reproduite pour des produits ou services identiques à ceux désignés dans l'enregistrement, la suppression ou la modification d'une marque.

L'utilisateur ne saurait utiliser une marque sur laquelle l'établissement ne détient pas l'autorisation expresse d'utilisation dans le cadre de ses fonctions.

Il lui sera en outre interdit d'utiliser à des fins privées toute marque dont l'établissement est titulaire.

Certaines inventions et autres créations sont susceptibles d'être protégées par le droit des dessins et modèles et le droit des brevets. Par conséquent, l'utilisateur s'interdit de les utiliser sans l'autorisation expresse de leurs titulaires.

ARTICLE VII. LA PROTECTION DES SYSTÈMES D'INFORMATION

La loi n°95-73 du 21 janvier 1995 modifiée en 2006 d'orientation et de programmation relative à la sécurité dispose que « la sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives ».

De même, la loi dite « Informatique et libertés » pose le principe selon lequel le responsable du traitement de données à caractère personnel est tenu de prendre toutes précautions, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données, et notamment d'empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Ces obligations pesant sur l'établissement justifient les règles de conduite et les interdictions édictées par le guide des utilisateurs.

Il est enfin rappelé qu'un usage non conforme peut être assimilé à une atteinte aux systèmes d'information, en tant que systèmes de traitement automatisé de données. Une telle atteinte relève de la réglementation sur la fraude informatique[17] qui sanctionne notamment :

- L'accès ou le maintien dans un système

L'accès illicite, c'est-à-dire toute pénétration dans un système d'information par une personne non autorisée, tel que la connexion pirate, tant physique que logique, l'appel d'un logiciel ou d'un fichier, alors que l'on ne dispose pas de l'habilitation pour le faire.

Le maintien frauduleux, c'est-à-dire le maintien au sein d'un système d'information, après un accès illicite et après avoir pris conscience du caractère « anormal » de ce maintien.

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende, (article 323-1 du Code pénal).

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende, (article 323-1 du Code pénal).

- L'entrave au fonctionnement

L'entrave du système, c'est-à-dire toute perturbation volontaire du fonctionnement d'un système d'information. L'entrave au système est appréhendée de manière extensive, car il suffit d'une influence « négative » sur le fonctionnement du système pour que l'entrave soit retenue. Il en est ainsi pour les bombes logiques, l'occupation de capacité mémoire, la mise en place de codifications, de barrages ou de tous autres éléments retardant un accès normal à un système d'information.

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende, (article 323-2 du Code pénal).

- L'altération des informations

[17] Art. 323-1 et suivants du Code pénal.

L'altération des informations est matérialisée par la suppression, la modification ou l'introduction de données pirates, avec la volonté de modifier l'état du système et ce, quelle que soit l'influence.
Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende, (article 323-3 du Code pénal).

- La détention de virus

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 du Code pénal est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Il en est ainsi pour les bombes logiques, l'occupation, la saturation de la capacité mémoire, la mise en place de codification, de barrage, ou tout autre élément retardant un accès normal.

Par ailleurs, la création de faux et leur usage, constitue un délit autonome sanctionné au titre de faux en écriture privée, publique ou de commerce.

L'utilisateur doit impérativement adopter un comportement exempt de toute fraude car à défaut, il s'expose à de sévères sanctions pénales et disciplinaires.
La Cour d'appel de Paris a par ailleurs précisé que l'existence d'une faille de sécurité ne constitue en aucun cas une excuse ou un prétexte pour l'auteur des faits d'accéder de manière consciente et délibérée à des données dont la non-protection pouvait être constitutive d'une infraction pénale[18].

ARTICLE VIII. LE SECRET DES CORRESPONDANCES

L'utilisateur est informé du caractère personnel et confidentiel des correspondances privées qui peuvent être échangées grâce aux ressources de télécommunication, au titre de l'utilisation de l'intranet et de l'accès à l'internet.

L'utilisateur est informé qu'est puni d'un an d'emprisonnement et de 45000 euros d'amende « le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination adressées à des tiers, ou d'en prendre frauduleusement connaissance , d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises ou transmises par la voie de télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions » (article 226-15 du Code pénal).

Il est également informé qu'est puni de trois ans d'emprisonnement et de 45000 euros d'amende, « le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances… »(article 432-9 du Code pénal).

S'agissant des agents publics, l'article 432-9 du Code pénal sanctionne « le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa fonction, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement,

[18] CA Paris 12e ch sect A 30-10-2002 Kitetoa c/ Tati SA.

la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances ».[19]

ARTICLE IX. UTILISATION DES SYSTEMES D'INFORMATION[20]

SECTION IX.1 SECURITE

L'utilisateur est informé des risques inhérents à l'utilisation d'internet, tout particulièrement en termes de :

- défaut de sécurité dans la transmission des données ;
- fiabilité relative des informations présentes sur le réseau ;
- continuité non garantie dans l'accès au service, en fonction de son encombrement, qui peut induire des temps de réponse extrêmement variables.

La sécurité des ressources informatiques et de télécommunication mises à disposition impose de :

- respecter les consignes de sécurité;
- respecter la gestion des accès, en particulier ne pas masquer sa véritable identité en se connectant sous le nom d'un autre utilisateur ;
- garder confidentiels ses mots de passe et ne pas les dévoiler à un tiers, sauf s'il s'agit d'un administrateur des systèmes d'information.

SECTION IX.2 MOYENS DE CRYPTOLOGIE

L'utilisateur est informé de la possibilité d'utiliser des moyens de cryptologie par l'établissement, sous réserve du respect des exigences et des conditions d'intégrité et de confidentialité fixées par l'établissement.

A ce titre, l'utilisateur est également informé que l'utilisation de tels moyens de cryptologie est strictement réglementée et que les règles édictées ont un caractère impératif, tant pour la sécurisation de l'utilisation et de l'intégrité du système, que pour la confidentialité des informations.

L'utilisation de moyens de cryptologie recouvre différentes fonctions :

- l'authentification des messages ;
- le respect de leur intégrité ;
- la confidentialité des messages ;
- la non-répudiation des messages émis, c'est-à-dire l'impossibilité de les remettre en cause.

La mise en oeuvre des systèmes de cryptologie est donc recommandée, tant au titre de la sécurité dans la transmission des informations que de la preuve de ces mêmes données.

Le régime juridique de la cryptologie est réglementé par la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique qui a rendu libre l'utilisation des moyens de cryptologie.

Le régime de la liberté d'utilisation des moyens de cryptologie n'existe pas dans tous les pays. L'utilisateur devra préalablement à toute importation de données cryptées dans un pays étranger vérifier le régime en vigueur pour éviter tout risque de confiscation desdites données.

[19] Une disposition spécifique applicable aux agents publics prévue à l'article 432-9 du Code pénal a été ajoutée.

[20] Cet article, en visant directement la messagerie des personnels rend le présent guide plus opérationnel en concernant directement un outil utilisé au quotidien par les personnels de l'établissement.

SECTION IX.3 AUDIT ET CONTROLE

La surveillance et le contrôle des salariés sur le lieu et pendant le temps de travail font partie des prérogatives reconnues à l'employeur, pour autant que les procédés utilisés ne soient pas illicites.

C'est dans ce cadre que s'inscrivent les audits et contrôles que peut être amené à réaliser l'établissement aux fins notamment de vérifier la conformité de l'usage des moyens informatiques et de communication électronique qu'il met à disposition.

En termes de traçabilité et de filtrage, l'utilisateur doit se conformer aux dispositions de la charte des systèmes d'information.

La jurisprudence de la Cour de cassation a jugé que l'employeur peut rechercher et identifier les sites internet sur lesquels un salarié a surfé pendant son temps de travail et le sanctionner sans que cela porte atteinte à l'intimité de sa vie privée[21]

Par un arrêt du 21 septembre 2011, la Cour de cassation a jugé qu'est constitutif d'une faute grave à ses obligations découlant du contrat de travail le fait pour un salarié d'avoir consulté des sites de rencontre et d'activité sexuelle sur son lieu de travail et d'avoir tenté d'effacer ses traces en téléchargeant un logiciel à cet effet[22]

Les fichiers électroniques clairement revêtus de la mention « PRIVE », peuvent être consultés par l'établissement en dehors de la présence de l'utilisateur mais en présence uniquement d'un risque ou d'un événement particulier ou, si un juge l'y autorise sur le fondement de l'article 145 du Code de procédure civile.

La Cour de cassation considère que le respect de la vie privée du salarié ne constitue pas en lui-même un obstacle à l'application de mesures d'instruction afin de conserver des preuves[23].

Ces audits et contrôles relèvent des compétences du personnel de la Direction informatique qui a la charge de la qualité et de la sécurité des services informatiques fournis aux utilisateurs. Le personnel de la Direction informatique gardera toutefois confidentielles les informations qu'il pourrait être amené à connaître à cette occasion.

L'établissement se réserve le droit, dans les conditions prévues par la charte des systèmes d'information, de mettre en place un autocommutateur ou PABX qui enregistre, à partir de chacun des postes téléphoniques fixes, les éléments de communication (date, heure, durée, cout et numéros appelés) ;

Les mêmes informations sont disponibles via les opérateurs téléphoniques pour les moyens informatiques et de communication électronique nomades (téléphone portable, BlackBerry, etc.).

La Cour de cassation a jugé que la simple vérification des relevés de la durée, du coût et des numéros des appels téléphoniques passés à partir de chaque poste édités au moyen

[21] Cass. soc 8-7-2009, dans cette affaire un informaticien consacrait, parfois, jusqu'à quatre heures par jour, à l'entretien d'une messagerie et à des consultations internet à des fins purement privées et ludiques. Il avait, en outre, sollicité l'informaticien sous ses ordres pour pouvoir se connecter anonymement sur internet, tout en ignorant que le numéro d'identification des machines restait enregistré. Or, l'utilisation privée d'une connexion internet d'entreprise doit rester « raisonnable », au même titre que le téléphone ou les photocopies, le salarié étant tenu d'une obligation de loyauté vis-à-vis de son employeur. En cas d'abus, la sanction peut être très sévère, comme en l'espèce, jusqu'au licenciement pour faute grave.

[22] Cass. soc 21-9-211, n°10-14869.

[23] Cass. soc. 23-5-2007 n°05-17818.

de l'autocommutateur téléphonique de l'établissement ne constitue pas un procédé de surveillance illicite, alors même que le salarié n'en avait été préalablement informé[24] ;

En revanche, ces dispositifs ne s'appliquent pas aux représentants du personnel.

La vidéosurveillance dite de « sécurité privée » est régie par :

- les principes directeurs de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, dans la mesure où les activités de vidéosurveillance ne sont pas visées en tant que telles, à la différence, par exemple, des technologies de biométrie ;

- la délibération n°94-056 du 21 juin 1994 portant adoption d'une recommandation sur les dispositifs de vidéosurveillance mis en œuvre dans les lieux publics et les lieux recevant le public. Cette disposition reste d'actualité, sous réserve des prescriptions de la loi n°95-73 d'orientation et programmation relative à la sécurité du 21 janvier 1995 et de la refonte de la loi Informatique et libertés par la loi du 6 août 2004.

Ces dispositions visent la prise de vue avec ou sans enregistrement de même que la connexion avec des fichiers nominatifs.

ARTICLE X. LA RESPONSABILITÉ EN MATIÈRE DE TRANSMISSION DES INFORMATIONS

Les moyens informatiques mis à la disposition de l'utilisateur permettent l'accès à une communication et à une information importante et mutualisée.

Or, de tels moyens de communication ne doivent pas permettre de véhiculer n'importe quelle information ou donnée, dès lors que celle-ci serait susceptible de mettre en péril des mineurs.

Ainsi, le Code pénal, dans ses articles 227-23 et 227-24, sanctionne le fait de fabriquer, de transporter, de diffuser, par quelque moyen que ce soit et quel qu'en soit le support, un message à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message de trois ans d'emprisonnement et de 75 000 euros d'amende. Est également puni de cinq ans d'emprisonnement et de 75 000 euros d'amende, le fait de fixer, d'enregistrer ou de transmettre en vue de sa diffusion, l'image ou la représentation d'un mineur lorsque cette dernière présente un caractère pornographique(…) ou d'inciter des mineurs à se livrer à des jeux les mettant physiquement en danger.

Est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende, « le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit ».

ARTICLE XI. LE RESPECT DE LA VIE PRIVEE

SECTION XI.1 LE DROIT A LA VIE PRIVEE

Le principe est posé par l'article 9 du Code civil qui prévoit que "chacun a droit au respect de sa vie privée".

La diffusion de toute information qui relève de la sphère privée d'une personne est susceptible d'engager la responsabilité civile de l'auteur de cette diffusion.

[24] Cass. soc. 29-1-2008 n°06-45279.

Par information qui relève de la sphère privée des personnes, il faut entendre notamment des informations portant sur la vie sentimentale d'une personne, sur ses mœurs sexuelles, sur sa famille ou encore sur sa rémunération.

Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre ou autres, propres à empêcher ou à faire cesser une atteinte à l'intimité de la vie privée ;

Cette notion de respect de la vie privée s'étend au droit à l'image et aucune image d'une personne ne peut être reproduite sans son autorisation préalable.

SECTION XI.2 DROIT À L'IMAGE ET CAPTATION

L'utilisateur est informé qu'est puni d'un an d'emprisonnement et de 45 000 euros d'amende, « le fait au moyen d'un procédé quelconque, de porter volontairement atteinte à l'intimité de la vie privée d'autrui :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur des paroles prononcées à titre privé ou confidentiel ;

2° En fixant, enregistrant ou transmettant sans le consentement de celle-ci l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés ci-dessus ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé ». (article 226-1 du Code pénal).

Par ailleurs, les personnes physiques bénéficient d'une autre protection au titre du droit pénal en application notamment de l'article 222-33-3 qui considère comme acte de complicité des atteintes volontaires à l'intégrité de la personne le fait d'enregistrer sciemment, par quelque moyen que ce soit, sur tout support que ce soit, des images relatives à la commission de ces infractions .

Le fait de diffuser l'enregistrement de telles images est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Le présent article n'est pas applicable lorsque l'enregistrement ou la diffusion résulte de l'exercice normal d'une profession ayant pour objet d'informer le public ou est réalisé afin de servir de preuve en justice ».

SECTION XI.3 LE DROIT DE REPRESENTATION

L'utilisateur est informé qu'est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention (article 226-8 du code pénal).

ARTICLE XII. LES RÈGLES DE PREUVE

En matière administrative, le principe est celui de la liberté de la preuve qui peut donc être rapportée par tout moyen.

A ce titre, l'utilisateur est informé qu'un message électronique peut constituer une preuve susceptible d'engager la responsabilité de l'établissement ainsi que la sienne.

En effet le code civil reconnaît à travers les articles 1316 à 1316-4 une valeur juridique à l'écrit sous forme électronique. De même les articles les articles 1369-1 et suivant du code civil reconnaissent une valeur juridique aux contrats sous forme électronique.

Il est nécessaire que chaque utilisateur respecte scrupuleusement la législation en vigueur car le non-respect de cette obligation est passible de sanctions pénales.

ARTICLE XIII. L'OBLIGATION D'INFORMATION

L'article 40 du code de procédure pénale précise que « Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs.

Il s'agit là d'une obligation forte attachée à la personne d'un fonctionnaire qui est tenu d'informer mais également de communiquer les éléments dont il dispose auprès du procureur de la République lorsqu'il à connaissance d'un crime ou d'un délit.

ARTICLE XIV. LIBERTÉ D'EXPRESSION ET SES LIMITES[25]

SECTION XIV.1 PRINCIPE DE LA LIBERTÉ D'EXPRESSION INDIVIDUELLE

Le principe de la libre communication des pensées et des opinions a été consacré notamment par l'article 11 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789.
La Convention européenne des droits de l'homme prévoit également un droit d'expression général en son article 10 alinéa 1.
Au niveau de l'entreprise, cette liberté est définie par le Code du travail et l'article L. 1121-1 qui dispose que « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ».

S'agissant des agents publics, l'article 6 de la loi du 13 juillet 1983 indique que la liberté d'opinion est garantie aux fonctionnaires.
Cette loi renvoie alors à la Déclaration des droits de l'homme et du citoyen de 1789 rappelant que le statut des fonctionnaires ne saurait s'opposer à cette déclaration.
Il existe cependant une obligation de réserve qui contraint les agents publics à observer une retenue dans l'expression de leur opinion, sous peine de s'exposer à une sanction disciplinaire, mais qui ne figure pas explicitement dans les lois statutaires relatives à la fonction publique[26].

L'article 433-5 du Code pénal prévoit et réprime l'infraction d'outrage envers une personne chargée d'un service public. Ainsi, constituent un outrage puni de 7500 euros d'amende les paroles, gestes ou menaces, les écrits ou images de toute nature non rendus publics ou l'envoi d'objets quelconques adressés à une personne chargée d'une mission de service public ou dépositaire de prérogatives de puissance publique, dans l'exercice ou à l'occasion de l'exercice de sa mission, et de nature à porter atteinte à sa dignité ou au respect dû à la fonction dont elle est investie.

[25] Il est proposé d'ajouter un thème sur la liberté d'expression et ses limites qui rappelle les principes fondamentaux en indiquant les limites à la liberté d'expression. En effet, les outils collaboratifs et les plateformes de communication collectives notamment à travers la participation à des services de type web 2.0 conduisent à la multiplication de tenues de propos pouvant porter atteinte à l'entreprise, l'organisme public, voire à des tiers, sources de responsabilité.
[26] Ces règles existent naturellement dans l'environnement numérique.

Les courriers électroniques adressés à cette personne constituent des écrits qui peuvent être sanctionnés au titre de l'outrage

SECTION XIV.2 LIMITES À LA LIBERTÉ D'EXPRESSION

La liberté d'expression n'est toutefois pas sans limite et toute personne peut engager sa responsabilité civile et/ou pénale à raison de la violation de certaines règles considérées comme ayant une portée équivalente.

Les délits par la voie de la presse ou tout autre moyen de communication

- La diffamation

Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation.
La publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable, même si elle est faite sous forme dubitative ou si elle vise une personne ou un corps non expressément nommés, mais dont l'identification est rendue possible par les termes des discours, cris, menaces, écrits ou imprimés, placards ou affiches incriminés.
La diffamation commise envers les particuliers sera punie d'une amende de 12 000 euros, (article 32, loi du 29 juillet 1881 sur la liberté de la presse).
La diffamation commise envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée sera punie d'un an d'emprisonnement et de 45 000 euros d'amende ou de l'une de ces deux peines seulement.
Sera punie des peines prévues à l'alinéa précédent la diffamation commise envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap.

- L'injure

Toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait est une injure, (article 33, loi du 29 juillet 1881).
L'injure commise envers les particuliers, lorsqu'elle n'aura pas été précédée de provocations, sera punie d'une amende de 12 000 euros.
Sera punie de six mois d'emprisonnement et de 22 500 euros d'amende l'injure commise envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée.
Sera punie des peines prévues à l'alinéa précédent l'injure commise envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap.

- La dénonciation calomnieuse

L'attention de l'utilisateur est attirée sur le fait que la dénonciation, effectuée par tout moyen et dirigée contre une personne déterminée, d'un fait qui est de nature à entraîner des sanctions judiciaires, administratives ou disciplinaires et que l'on sait totalement ou partiellement inexact, lorsqu'elle est adressée :

- soit à un officier de justice ou de police administrative ou judiciaire,
- soit à une autorité ayant le pouvoir d'y donner suite ou de saisir l'autorité compétente,
- soit aux supérieurs hiérarchiques ou à l'employeur de la personne dénoncée,

est punie de cinq ans d'emprisonnement et de 45 000 euros d'amende, (article 226-10 du Code pénal).

La fausseté du fait dénoncé résulte nécessairement de la décision, devenue définitive, d'acquittement, de relaxe ou de non-lieu déclarant que la réalité du fait n'est pas établie ou que celui-ci n'est pas imputable à la personne dénoncée.

SECTION XIV.3 SANCTIONS

Les sanctions encourues sont celles prévues dans les dispositions suivantes :

- loi du 29 juillet 1881 sur la liberté de la presse, articles 32 et 33.
- article 226-10 du Code pénal.

Les peines applicables sont des peines de prison allant de 6 mois à 5 ans d'emprisonnement, et des peines d'amende allant de 12 000 à 45 000 euros.

ARTICLE XV. RESPONSABILITÉ ET SANCTIONS

Dans le cadre de son activité professionnelle, l'utilisateur engage sa responsabilité en ne se conformant pas aux termes de la charte des systèmes d'information.

En cas de non-respect de la charte, celui-ci s'expose à des sanctions civiles, pénales et disciplinaires s'agissant des salariés.

ARTICLE XVI. MISE À DISPOSITION DU GUIDE JURIDIQUE ET ÉVOLUTIONS

Le présent guide est mis à la disposition des utilisateurs sur l'Intranet de l'établissement.

Le présent guide sera régulièrement mis à jour et il appartient à l'utilisateur de prendre connaissance de toute nouvelle version du guide qui sera portée à sa connaissance par le biais de l'Intranet.

Une information sera communiquée à l'ensemble des utilisateurs à chaque nouvelle version du guide.