CHARTE D'USAGE

DES SYSTEMES D'INFORMATION

La présente charte définit les règles d'usage et de sécurité du système d'information que la Collectivité met à la disposition de l'ensemble des utilisateurs quelque soit son statut.

Les droits d'accès aux ressources informatiques de la Collectivité ne sont octroyés qu'après l'engagement de respecter la présente charte et pourront être suspendus ou retirés dès lors que l'utilisateur dérogera à ces obligations ou enfreindra la loi.

Les « systèmes d'information » de la Collectivité sont composés de l'ensemble des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition ou pouvant être apporté par l'utilisateur, après accord et validation de la présente charte.

Sommaire

Article 1 : Règles générales d'utilisation des ressources du système d'information

Ce règlement s'applique à tout utilisateur quelque soit son statut ou sa fonction et quelque soit le niveau d'utilisation de la ressource utilisée appartenant à la collectivité. Tout utilisateur est responsable de l'utilisation qu'il fait des ressources du système d'information et s'engage à ne pas effectuer d'opération susceptible de porter atteinte de quelque façon que ce soit :

- à l'intégrité, la sécurité, la disponibilité du système d'information de la Collectivité ;
- à l'image de la Collectivité ;
- au respect de la vie privée, au droit à l'image, au droit d'auteurs et droits voisins de toute personne physique ou morale, privée ou publique ;
- à l'ordre et à la sécurité publique ;
- aux biens et personnes par des faits constitutifs d'infractions pénales.

Accès aux systèmes d'information : L'utilisation des ressources informatiques de la Collectivité, supposant l'approbation de la présente charte, est soumise à autorisation préalable. Elle peut être retirée, partiellement ou totalement, temporairement ou définitivement, en cas de non respect de la charte.

Le droit d'accès aux ressources informatiques est **personnel** et **incessible**. Il disparaît dès que son utilisateur ne remplit plus les conditions qui lui ont autorisé l'accès.

Usages des systèmes d'information : Les moyens informatiques de la Collectivité mis à la disposition des utilisateurs sont destinés à une utilisation dans le cadre professionnel. Il devra être fait un usage raisonnable, non susceptible d'amoindrir les conditions d'accès professionnel aux ressources, ne mettant pas en cause la productivité de la Collectivité.

L'utilisation d'équipements ou de logiciels non fournis ou non approuvés par le service des Systèmes d'Information de la Collectivité engage la responsabilité de l'utilisateur et ne peut être tolérée que si :

- Il ne peut être trouvé de solutions de contournement ;
- La légalité de l'utilisation est incontestable ;
- La disponibilité, l'intégrité et la confidentialité des systèmes d'information sont préservées.

Une adresse électronique « @ccbrianconnais.fr » est attribuée à tout utilisateur qui en ferait la demande. La plus grande correction doit être respectée dans les échanges électroniques. Les contenus doivent être conformes aux lois et règlements en vigueur (Cf. article 3.2 de la présente charte sur la messagerie électronique). La Collectivité utilisera exclusivement cette adresse pour tous les échanges officiels.

Usages personnels des systèmes d'information : L'utilisation résiduelle du système d'information à titre privé est tolérée sous réserve qu'elle soit éthique, licite, non lucrative, conforme à la présente charte et raisonnable en termes de fréquence et de durée.

Conformité aux lois et règlements : L'utilisateur s'engage à un usage des systèmes d'information de la Collectivité conforme aux lois et règlements en vigueur, notamment en ce qui concerne la propriété intellectuelle, la diffusion de l'information, le droit à la vie privée et la loi informatique et libertés.

Article 2 : Rappel des principales dispositions légales eu égard à l'objet de la présente charte

L'utilisateur s'engage à ne commettre aucune infraction aux dispositions légales et réglementaires en vigueur, notamment :

- La législation relative à la protection des systèmes informatiques notamment les articles 323-1 à 323-7 du Code Pénal :

• 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 30 000 euros d'amende. 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 45 000 euros d'amende ;

• 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 75 000 euros d'amende ;

• 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 ;

• La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

Les personnes physiques coupables des délits prévus au présent chapitre encourent également des peines complémentaires, notamment l'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, et l'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.

- La législation relative à la protection des droits de propriété intellectuelle notamment les articles L335-1 à 335-10 du Code de la propriété intellectuelle :

Les dispositions interdisent notamment à tout utilisateur de réaliser des copies de logiciels commercialisés, pour quelque usage que ce soit, ainsi que de dupliquer, distribuer ou diffuser des documents (images, sons, vidéos,...) protégés, ou d'altérer la protection d'une œuvre, d'un phonogramme, d'un vidéogramme ou d'un programme par un décodage, un décryptage ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle.

- La législation relative à la protection des données à caractère personnel, notamment les articles 50 à 52 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés :

Les infractions aux dispositions de la loi de 1978 sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

- Les autres références réglementaires et législatives sont consultables en annexe. La liste n'est pas exhaustive compte-tenu de son caractère législatif.

Article 3 : Règles de fonctionnement

3.1 Sécurité des accès – règles élémentaires

Conformément à la politique de sécurité des systèmes d'information de la Collectivité, la protection des ressources mises à la disposition de l'utilisateur nécessite l'application d'un certain nombre de règles élémentaires :

• Choisir un mot de passe complexe[1], le garder strictement confidentiel et demander sa modification en cas de doute sur sa confidentialité ; utiliser des mots de passe différents pour accéder à des environnements différents (sites institutionnels, sites commerciaux, réseaux sociaux...) ou une technologie équivalente hautement sécurisée ;

• Respecter la gestion des accès, en particulier ne pas utiliser les mots de passe d'un autre utilisateur, ni chercher à les connaître[2] ;

• Ne pas tenter d'accéder à des ressources du système d'information, à des informations détenues par d'autres utilisateurs et aux communications entre tiers pour lesquelles il n'a pas d'autorisation explicite. Il faut noter que la capacité d'accéder à une information n'implique pas que l'accès soit effectivement autorisé ;

• Ne pas rendre accessibles à des tiers les services qui lui sont offerts dans le cadre professionnel sans y être dûment autorisé ;

• Ne pas publier des documents de la Collectivité auxquels il a accès dans le cadre professionnel, sous quelque forme que ce soit, sans y être dument autorisé ;

• Se conformer aux dispositifs mis en place ou autorisés par la Collectivité[3] pour lutter contre les virus et les attaques par programmes informatiques et se conformer aux recommandations des administrateurs des systèmes informatiques ;

• Signaler aux **gestionnaires du système d'information** toute anomalie ou dysfonctionnement des systèmes informatiques, notamment tout ce qui concerne la sécurité ;

• Ne pas nuire volontairement au bon fonctionnement des ressources informatiques et des réseaux par des manipulations anormales du matériel ou par l'introduction de logiciels malveillants ou intrusifs (virus, chevaux de Troie, bombes logiques, outils d'intrusion...) ;

• **Enfin, ne jamais quitter son poste de travail sans verrouiller ou fermer sa cession.**

[1] Minimum 10 caractères, mélange de lettres majuscules et minuscules, de chiffres et, si possible, de caractères spéciaux, paraissant aléatoire ou dénué de sens pour tout autre personne que son propriétaire (voir par exemple http://www.securite-informatique.gouv.fr/autoformations/motdepasse/co/Mots_de_Passe_CH01_SCH02.html).

[2] **À noter que l'hameçonnage (« phishing » en anglais) est une méthode courante pour obtenir frauduleusement un mot de passe.** Toute demande de mot de passe par courriel (avec réponse par le même canal ou en suivant un lien vers un formulaire web) est illégitime ; aucune suite ne doit y être donnée ; **en cas de doute vous devez contacter le gestionnaire du système d'information.**

[3] La Collectivité **validera avec l'utilisateur**, en cas de matériel personnel « apporter » par ce dernier, connu aussi sous le nom de BYOD (Bring Your Own Device), **l'efficacité de sa protection antivirale et pare-feu**, les mises à jour antivirus et de sécurité du système **d'exploitation. En cas de refus de mise en conformité et de suivi des préconisations de la Collectivité, l'accès aux ressources du système d'information sera purement et simplement refusé à l'utilisateur.**

3.2 Messagerie électronique

3.2.1 Principes d'utilisation

La messagerie électronique est un moyen de communication omniprésent et spécifique car c'est un outil de communication rapide, écrit, asynchrone, à un ou plusieurs interlocuteurs et comportant une mémoire externe. Il convient donc d'encadrer au sein de la Collectivité son utilisation. Les utilisateurs veilleront donc à :

- S'interroger sur la pertinence de l'utilisation de la messagerie électronique au regard des autres outils de communication (face à face, téléphone, visioconférence, courrier ...) ;
- Favoriser les échanges directs lorsque les niveaux de compréhension et d'interaction sont élevés ou lorsque celui-ci est potentiellement conflictuel ;
- Aborder un seul et unique sujet au sein d'un même message. Cela évite les pertes d'informations, les messages partiellement consultés ou d'importuner des destinataires avec de l'information ne les concernant pas directement ;
- Indiquer le sujet précis et unique dans le champ « objet » du message. Cela évite au destinataire toute perte de temps dans le traitement du message ;
- Ne pas abuser des pièces jointes et s'interroger sur la pertinence de leur envoi (taille du fichier, compatibilité ...) ;
- Utiliser avec modération les destinataires en copie : un destinataire en copie ne donne aucune garantie que votre message soit pris en compte !
- S'interroger sur l'heure d'envoi du message et sur les délais qui peuvent être nécessaires à sa prise en compte ;
- Adopter les mêmes règles de rédaction que le courrier « manuscrit » : Identifier l'expéditeur et le destinataire, éviter les tournures trop personnelles ou familières, éviter le langage parlé, éviter

l'utilisation abusive des mots en majuscule (agressif), gras ou italique, veiller à l'orthographe et aux formules de politesse.

3.2.2 Engagement vis à vis des tiers

Un message électronique peut être une preuve ou un début de preuve. Ainsi, en matière commerciale, une preuve peut être apportée par tous les moyens possibles. De plus, en droit commercial, il y a contrat dès lors que les parties ont donné leur accord sur la chose et sur le prix. Ainsi, une proposition chiffrée émise par un offreur puis acceptée par un client constitue de fait un contrat, sans que la mention explicite et formelle "Contrat" soit nécessaire.

Il existe donc un risque réel qu'un agent prenne par messagerie des engagements sans qu'il ait reçu délégation. Le caractère fugace des messages électroniques crée une fausse impression de sécurité.

Il est donc rappelé que toutes les recommandations concernant les échanges écrits avec des tiers s'appliquent à la messagerie, et notamment la transmission pour validation à un responsable ayant délégation tout message qui aurait valeur contractuelle ou d'engagement.

3.2.3 Comportement / actes illicites

Il est interdit aux utilisateurs de stocker, transférer ou diffuser des documents proscrits par la loi, et notamment les documents à caractère raciste, négationniste, ou pornographique. Certes, un agent ne peut être tenu pour responsable s'il reçoit, à son insu, de tels documents, mais il lui est imposé de les détruire et de ne pas les diffuser.

Il ne doit donc pas en solliciter l'envoi en participant à des groupes de discussion, ou en consultant des sites internet, dont le caractère est proscrit et qui pourraient enregistrer ses coordonnées.

3.2.4 Conservation des messages

Il est conseillé d'employer les mesures suivantes afin de se prémunir contre toute perte d'information :

- Enregistrer les pièces jointes à conserver sur un autre support (ex : serveur de partage de fichiers) ;
- Supprimer rapidement tous les messages volumineux et sans valeur contractuelle, afin de ne pas engendrer de coût de stockage pour de l'information inutile.

Il est demandé de conserver et de classer dans la boite professionnelle :

- Les mails contenant des informations qui engagent la Collectivité ou qui peuvent être opposées à la demande d'un tiers.
- Les mails contenant des informations pouvant être utiles au bon fonctionnement de la Collectivité.

3.2.5 Sécurité

Les supports de stockage externes (disques durs, clés USB) et la messagerie sont devenus les premiers vecteurs de propagation des virus. Il est en effet très simple de diffuser, sous forme de fichier attaché par exemple, un programme infecté.

Des outils ont été mis en place pour prémunir la Collectivité contre ce type d'attaque. Toutefois il est impossible de garantir un niveau de sécurité totale, il est donc nécessaire de respecter les précautions simples décrites ci-dessous:

- Les fichiers rattachés ayant une extension de type ".exe" ne doivent jamais être ouverts. Il est indispensable de prévenir le service informatique pour analyse, ou de les supprimer directement.
- Les messages suspects (ayant un objet douteux, provenant d'un émetteur inconnu, ayant une pièce jointe inhabituelle, ...) ne doivent pas être ouverts et directement transmis au service informatique pour analyse ou destruction.

En outre, et afin d'assurer un niveau de sécurité maximum, il est strictement interdit de désactiver les systèmes de protection du poste de travail mis à la disposition des agents.

3.2.6 Utilisation de la messagerie électronique à des fins personnelles

Il est considéré que tout message reçu ou envoyé à partir du poste de travail mis à la disposition de l'utilisateur revêt par principe un caractère professionnel.

L'utilisation de la messagerie à des fins personnelles n'est tolérée qu'a titre exceptionnel ou par les impératifs de la vie courante et familiale, et dès lors qu'elle n'affecte pas le trafic normal de la messagerie professionnelle.

Le message qui comportera la mention expresse ou manifeste de son caractère personnel, bénéficiera du droit au respect de la vie privée et du secret des correspondances.

Cependant, l'utilisateur doit être informé du fait que toute activité numérique, comme l'utilisation de la messagerie électronique, laisse des traces et donc, est nécessairement mémorisée.

L'utilisateur est informé que pour des raisons de sécurité, d'organisation ou de gestion de l'encombrement du réseau, le service informatique peut mettre en place des dispositifs d'analyse de messages ou des dispositifs visant à limiter la taille ou le volume des messages échangés.

Si des anomalies étaient détectées, des mesures de contrôle individuel par poste pourraient être mises en place après information collective et préalable des utilisateurs.

3.3 Accès internet

Seuls ont vocation à être consultés les sites Internet ayant un lien direct et nécessaire avec l'activité professionnelle et présentant une utilité au regard des missions et des fonctions à exercer.

Une consultation ponctuelle des sites Internet dont le contenu n'est pas contraire à l'ordre public et qui ne mettrait pas en cause les intérêts de la Collectivité, les règles statutaires et déontologiques, est tolérée. Néanmoins, comme le rappel la CNIL, il devra en être fait un « **usage raisonnable, non susceptible d'amoindrir les conditions d'accès professionnel au réseau et ne mettant pas en cause la productivité** ».

En conséquence, l'utilisateur s'engage expressément à respecter :

- Les Lois et Règlements en vigueur sur le territoire français et notamment de manière non limitative ceux régissant le fonctionnement des services en ligne, le commerce, la vente à distance, la protection des mineurs, le respect de la personne humaine et de la vie privée, la propriété intellectuelle ;
- Il s'interdit de stocker, diffuser ou rendre accessible de quelque façon que ce soit, tout message dont le contenu serait contraire notamment à la dignité humaine, à l'ordre public et aux bonnes mœurs, ou constituant une injure, de la diffamation, une incitation à la pédophilie, à la haine raciale, au meurtre, au terrorisme, au proxénétisme, au trafic de stupéfiants, à la contrefaçon notamment par fournitures de moyens illicites, au piratage informatique, ou susceptible de constituer une atteinte à la sécurité nationale.

Il est également rappelé que des utilisations contrevenant aux règles ci-dessus énoncées, sont susceptibles d'engager la responsabilité civile et/ou pénale de la Collectivité, outre bien évidemment celle de l'utilisateur.

Les utilisateurs sont informés que toutes les connexions internet sont susceptibles d'être identifiées par leur login et stockés pendant une durée maximale d'un an.

Le service informatique se réserve la possibilité de restreindre de manière automatique l'accès aux sites internet, et notamment ceux encombrant inutilement le réseau.

3.4 Utilisation du matériel informatique et téléphonique mis à disposition des utilisateurs

Tout utilisateur s'engage à ne pas effectuer d'opérations qui pourraient avoir pour conséquence :

- De modifier le fonctionnement, le paramétrage et les caractéristiques de son poste de travail informatique (installation de nouveaux matériels, de logiciels même gratuits, modification des fichiers systèmes, de la résolution d'écran, installation d'imprimantes, de modems,...) ;

- De modifier des éléments de configuration fournis, dans des limites portant atteinte aux performances du poste de travail ;
- D'interrompre, même temporairement, le fonctionnement de tout système connecté au réseau (le déplacement de tout matériel informatique ou téléphonique doit être réalisé par un agent du service informatique ou par une personne expressément habilitée ou à défaut avec l'accord du service informatique ;
- D'accéder ou d'essayer d'accéder à des informations privées d'autres utilisateurs du réseau ;
- De modifier ou de détruire des informations communes (partagées par plusieurs utilisateurs) stockées sur le réseau.

Il est expressément rappelé que l'accès à des informations privées d'autres utilisateurs, leur éventuelle destruction ou modification, sont des agissements pénalement sanctionnés.

La destruction ou la modification de documents élaborés par la Collectivité sans autorisation (Code du patrimoine, livre 2 art L212 et suivants) constitue également un agissement pénalement sanctionné.

L'utilisation des équipements informatiques et téléphoniques de la Collectivité est limitée à un usage professionnel. L'utilisation à titre privé est tolérée mais doit être très occasionnelle et sous réserve qu'elle ne perturbe pas l'activité professionnelle du service ou que cette utilisation ne représente pas un délit au regard de la législation.

L'encadrement pourra proposer à l'autorité territoriale de sanctionner tout utilisateur ayant une utilisation abusive des moyens informatiques (accès à des sites Web non professionnels, impression de documents personnels,...) ou téléphoniques.

Concernant la téléphonie fixe ou mobile, les utilisateurs sont informés qu'un relevé détaillé des consommations est disponible en consultation pour chaque responsable du service concerné.

Lorsque celui-ci relève une anomalie, il peut obtenir un relevé des consommations du poste (avec masquage des quatre derniers chiffres des numéros appelés) et solliciter des explications auprès du titulaire du poste. Le service informatique procède à des contrôles réguliers et peut, selon les mêmes procédés, saisir la Direction Générale de toute anomalie.

3.5 Installation de logiciels

L'utilisateur ne peut installer un logiciel (qu'il soit payant ou gratuit), que ce soit par copie ou téléchargement, sans l'accord express du service informatique et sous réserve d'une validation préalable d'opportunité formalisée par son responsable de service.

Aucune copie de logiciels n'appartenant pas au domaine public (respect du droit de propriété) n'est autorisée en dehors des copies de sauvegarde. L'utilisation et la diffusion de logiciels piratés constituent un délit passible d'amendes et d'emprisonnement.

Sa détention et sa diffusion correspondent à du recel.

3.6 Données informatiques

Le service informatique a le devoir d'assurer le bon fonctionnement des réseaux et des moyens informatiques.

Pour ce faire, il prend toutes dispositions nécessaires pour assumer cette responsabilité, tout en respectant la déontologie professionnelle.

Le service informatique peut ainsi effectuer des contrôles techniques sur les données informatiques du système dont il a la charge :

- Soit dans un souci de sécurité du réseau et/ou des ressources informatiques, pour des nécessités de maintenance et de gestion technique. L'utilisation des services et notamment des ressources

matérielles et logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment dans le respect des règles relatives à la protection de la vie privée et au respect des communications privées ;

- Soit dans un souci de vérification que l'utilisation des moyens informatiques et de télécommunications reste conforme aux règles édictées par la présente charte.

Article 4 : Mesures de contrôle de la sécurité

L'utilisateur est informé que :

- La Collectivité met en œuvre les mécanismes de protection appropriés sur le système d'information mis à la disposition des utilisateurs ;
- La Collectivité exerce une surveillance et un contrôle de son système d'information à des fins de sécurité et de détection des abus, de statistiques d'usage et d'optimisation des ressources, dans le respect de la législation applicable ;
- Conformément à la législation en vigueur[4] en termes de traçabilité, la Collectivité a mis en œuvre un système de journalisation (logs) des sessions des utilisateurs de son système d'information. La gestion des journaux informatiques est conforme aux règles énoncées dans un document spécifiques et à leur déclaration auprès de la CNIL. Un extrait de ces journaux, en rapport avec l'objet d'une enquête en cours, peut être remis à l'autorité judiciaire à sa demande ;
- La Collectivité se réserve le droit de limiter la diffusion et le téléchargement massifs de fichiers et courriers électroniques dès lors que cela peut être attentatoire à la sécurité du système d'information, à la responsabilité juridique de l'établissement et à son image ;
- Toute donnée bloquante pour le système ou générant une difficulté technique sera isolée ; le cas échéant supprimée ;
- En cas d'incident, la Collectivité se réserve le droit, avec information au plus tôt des utilisateurs, de filtrer ou d'interdire l'accès à certains sites ou l'usage de certains protocoles de communication.

Les personnels de la Collectivité chargés des opérations de contrôle du système d'information sont soumis à l'obligation de discrétion et au devoir de réserve. Cependant ils doivent communiquer les informations aux autorités compétentes si elles tombent dans le champ de l'article 40 alinéas 2 du code de procédure pénale[5].

En dehors de ces gestionnaires, seules les personnes habilitées par la loi à les obtenir, notamment les autorités judiciaires dans le cadre d'une procédure pénale, ou la Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet (HADOPI) peuvent demander la communication de ces données.

[4] Loi n° 2004-575 du 21 juin 2004 dite « pour la confiance dans l'économie numérique » (LCEN).

[5] Obligation faite à tout fonctionnaire d'informer sans délai le procureur de la République de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions.

Article 5 : Sanctions

En cas de non-respect des règles définies dans la présente charte, le Président de la Collectivité pourra par mesure conservatoire, sans préjudice des poursuites civiles ou pénales et des procédures disciplinaires pouvant être engagées à l'encontre de l'utilisateur, prendre toute mesure utile à la préservation de ses intérêts et des intérêts des personnels, usagers, partenaires publics et privés, ou tiers, notamment :

- Limiter les usages du système d'information ;
- Interdire tout accès au système d'information de la Collectivité ;

- Procéder à toute mesure d'investigation sur les ressources informatiques matérielles et immatérielles mises à disposition par la Collectivité ainsi que dans les échanges avec l'extérieur.

La Collectivité est également tenue par la loi de signaler aux services répressifs compétents toute violation des lois constatée.

En cas d'atteinte à l'un des principes protégés par la loi, la responsabilité pénale ou civile de l'utilisateur ainsi que celle de la Collectivité est susceptible d'être recherchée.

Toute infraction aux règles internes décrites dans le présent document peut entraîner des sanctions disciplinaires.

Article 6 : Opposabilité de la présente charte

La présente charte est rendue opposable dès sa notification à chaque utilisateur valant acceptation entière de ses termes.

Annexes : Références réglementaires et législatives

- Obligations de transparence et de concertations -

Décret de 1982 régissant les obligations de consulter le CTP.

Art. L 432-2 du code du travail prévoyant la consultation obligatoire du CTP lorsque l'employeur projette d'introduire dans l'entreprise des moyens qui rendent possible la surveillance des salariés.

Art. L 412-8 du code du travail modifié par l'article 45 de la loi relative à la formation professionnelle tout au long de la vie et au dialogue social, adoptée le 7 avril 2004. La nouvelle rédaction de cet article ne procure aucun droit nouveau en matière de communication syndicale sur les outils électroniques de l'entreprise.

- Responsabilité de la Collectivité -

Art. 1384 alinéas 5 du code civil prévoyant la responsabilité civile de l'employeur en cas de dommage causé par ses préposés dans les fonctions auxquelles il les a employés.

Art. L 120-2 du code du travail : "Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché".

Art. L 121-8 du code de travail (directement issu de la Loi du 6/1/78 dite "informatique et liberté") aux termes duquel "aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collecté par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi."

- Cadre législatif -

Loi du 29 juillet 1881 modifiée relative à la liberté de la presse (notamment chapitre IV : Des crimes et délits commis par la voie de la presse ou par tout autre moyen de publication).

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi 2004-801 du 6 août 2004 (cf. articles 226-16 à 226-24 et R625-10 du code pénal).

Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique dite "loi Godfrain" (cf. articles 323-1 à 323-7 du code pénal).

Code pénal, notamment les articles 226-1 et suivants relatifs à l'atteinte à l'intimité de la vie privée, les articles 226-15 et suivants relatifs au secret des correspondances, l'article 227-23 relatif à la détention et/ou la diffusion de documents à

caractère pédophiles et l'article 227-24 relatif à la diffusion et/ou au commerce de messages à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine.

Code Civil, notamment les articles relatifs au droit à l'image et à la protection de la vie privée.

Loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur, a étendu aux logiciels en tant qu'œuvres de l'esprit, la protection prévue par la loi n° 57-298 du 11 mars 1957 sur la propriété littéraire et artistique. (cf. Code de la Propriété Intellectuelle, œuvres définies par l'article L112-2, articles L335-2 et suivants sur la contrefaçon des œuvres de l'esprit, article L521-1 et suivants sur la contrefaçon des dessins ou modèles nationaux, article L713-1 et suivants sur la protection des marques).

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et le décret n° 2011-219 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

Loi n° 2009-669 du 12 juin 2009 a créé l'HADOPI chargée 1) de protéger les œuvres à l'égard des actes de contrefaçon numérique 2) d'encourager le développement de l'offre légale et observer l'utilisation licite et illicite des œuvres 3) d'assurer une régulation et une veille dans le domaine des mesures techniques ; complétée par la loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet.

Dernière mise à jour : Juin 2013

Déclaration de l'utilisateur

Je soussigné(e) *Nom, Prénom* ..... , certifie avoir pris connaissance de la présente charte et m'engage à m'y conforter sans restrictions.

Je certifie également avoir pris connaissance de mon droit d'accès et de rectifications aux informations personnelles détenues par la Collectivité, conformément aux articles 38 à 43 de la loi n°78-17 du 6 janvier 1978 modifiée.

Mention manuscrite « Lu et approuvé » : .....

Lieu, date : .....

Signature

Fait en double exemplaire : un exemplaire à conserver par l'intéressé, un exemplaire à remettre au service Ressources Humaines.