

# A vos chartes! Prêts? Partez!

## Encadrer l'usage du système d'information

**AVERTISSEMENT** La consultation du présent dossier ne saurait remplacer un entretien privé avec un conseil, qui seul est en mesure d'apporter une réponse précise à vos questions et à vous fournir une consultation

complète. Aquitaine Europe Communication ne saurait donc être considérée comme responsable de toute utilisation qui pourrait être faite du présent dossier et de son contenu, de quelque façon que ce soit.

### Pourquoi une charte ?

L'administration électronique et le développement des usages liés à l'informatique au sein des collectivités territoriales (intranet, applications informatiques, Courriel, badge électronique) modifient profondément les habitudes de travail des agents. De multiples structures (mairies, écoles, crèches, bibliothèques, théâtres, centres administratifs, police municipale...) peuvent dès lors communiquer entre elles de manière continue et sécurisée.

Chaque agent dispose, en plus de son ordinateur, d'un compte d'accès au système d'information de la collectivité et, pour ceux qui n'ont pas de bureau, des ordinateurs sont installés dans les lieux de passage comme la cantine ou certains centres techniques. Des documents de référence, actualités sur Internet, revue de presse, archives, agendas partagés sont dès lors disponibles aux agents qui peuvent également communiquer entre eux, par Courriel notamment.

Cette forteresse numérique contient donc des informations personnelles des agents touchant leur vie privée ; et par ailleurs certains usages personnels pourraient se révéler en contradiction avec la bonne administration de la collectivité.

Dans ce cadre, comment concilier le droit à un îlot de vie privée des utilisateurs au sein de leur activité avec le bon fonctionnement d'un service public (continuité et permanence du service public) ?

Il est donc apparu indispensable de rédiger des codes de bonnes pratiques ou chartes visant à prévenir les risques liés à une utilisation inappropriée d'une

ressource apportée par la collectivité à son personnel et à sensibiliser les utilisateurs, à leur faire prendre clairement conscience de ce à quoi ils s'engagent en se servant du système d'information au sein de leur établissement, c'est-à-dire dans une configuration notablement différente de celle d'un usage privé.

Une charte doit pouvoir informer les utilisateurs sur les caractéristiques des outils de communication proposés et sur les risques Courus. Elle doit former et éduquer les utilisateurs, mais aussi les mettre face à leurs responsabilités le cas échéant. La charte doit donc accompagner des citoyens numériques avec des valeurs et des comportements adaptés.

Tel est le but de la démarche qui encadre la mise en place des nouveaux outils de communication informatiques au sein d'une collectivité territoriale.

L'objectif de ce dossier de veille est de vous permettre à l'aide d'un conseil approprié de pouvoir rédiger une charte du système d'information de votre collectivité si ce n'est pas encore fait. Ce dossier est un donc un fil d'Ariane qui vous éclairera dans les dédales d'un édifice juridique obscur et difficile à appréhender.

### La mode des chartes

La charte est un instrument juridique pratique afin de cadrer des phénomènes pour lesquels aucune loi spécifique n'apporte de réponse. De nombreux domaines, dont l'éducation, ont vite vu les avantages de flexibilité et d'adhésion que présentaient ces codes de bonne conduite.

Dans le cas d'un système d'information, aucun cadre juridique spécifique n'existe

proprement dit. En fait, le cadre est protéiforme dans le sens où il va piocher dans différents corpus juridiques : loi pour la confiance dans l'économie numérique du 21 juin 2004, loi du 9 juillet 2004 relative aux communications électroniques, loi du 6 janvier 1978 modifiée par la loi du 6 août 2004, article L120-2 du code du travail, code de la propriété intellectuelle, code pénal (article 226-15) en ce qui concerne la fraude informatique (voir également les dispositions pénales de la loi Godfrain), code de la fonction publique et dispositions de l'article 10 du décret du 25 octobre 1984 relatif à la procédure disciplinaire concernant les fonctionnaires de l'Etat, code général des collectivités territoriale... La rédaction de la charte implique donc une compétence juridique globale et structurante incluant différentes dimensions (délégations de pouvoir et organisation interne, règles de la fonction publique, administrative, civile et pénale, en matière de sécurité informatique, libertés individuelles).

### Encadrer la cybersurveillance

La charte reflètera la position de la jurisprudence en la matière. La plupart des cas concernent des salariés du secteur privé.

Le problème n'est pas nouveau puisque les juges ont déjà été amenés à se prononcer sur des cas similaires à l'utilisation d'Internet avec l'utilisation des téléphones professionnels à des fins personnelles.

En ce qui concerne la surveillance des Courriels d'un employé, un arrêt de référence « Nikon » de la chambre sociale de la Cour de cassation du 2 octobre 2001 a détaillé la très forte



Rédacteur(s) :  
**François Gilbert**  
Rédaction initiale :  
14 octobre 2005



REGION



AQUITAINE

protection donnée à la correspondance électronique privée (Courriel) du salarié, en faisant référence au secret des correspondances.

Cependant, les juges, au fur et à mesure des décisions, affinent leurs raisonnements et rappellent que la vie privée au travail n'est pas sans limites. Pour preuve, le 17 mai 2005, à propos de la surveillance d'un disque dur et notamment de dossiers personnels, qui n'étaient pas nécessairement du Courriel électronique (vidéos, photos...), la Cour de cassation a énoncé le principe que l'employeur ne peut ouvrir les fichiers personnels du salarié qu'en présence du salarié ou une fois celui-ci dûment appelé.

Une exception à ce principe en cas de risque ou d'événement particulier. Cette condition sera interprétée de manière stricte et limitée à des cas graves : pédophilie, risque terroriste ou plus généralement « impératif immédiat de sécurité », en tant que risque informatique (virus par exemple) et risque de toute éventuelle utilisation détournée du système d'information qui porterait atteinte au fonctionnement global du système.

Dernier cas, les abus sont en général réprimés par la Cour de cassation qui

électronique nominative de son directeur de laboratoire pour communiquer sur le site de la secte Moon. Sans violer le secret des correspondances (argument utilisé dans l'arrêt Nikon), ce comportement a porté préjudice au directeur du laboratoire et à l'établissement public dans lequel le technicien travaillait. La sanction disciplinaire est alors justifiée car le fonctionnaire a manqué à son obligation de laïcité en laissant les coordonnées de son supérieur sur le site concerné ayant un caractère religieux. Les abus manifestes seront donc sanctionnés. L'interdiction totale ne pouvant être effective, les chartes constituent l'outil idéal pour aménager une utilisation raisonnable du système d'information.

## Fixer le cadre

### Un objet volontairement large

Le système d'information irrigue toutes les activités de la collectivité. L'objet sera donc d'indiquer le noyau dur de cette convention. C'est-à-dire de formaliser des règles de déontologie et de sécurité que les utilisateurs s'engagent à respecter en contrepartie de la mise à disposition des ressources du système

intégrante du système. La définition fonctionnelle du système permettra de cadrer les éventuelles évolutions du système d'information. Il sera important de prévoir dans la charte des dispositions spécifiques au cas où les agents pourraient avoir accès aux données internes de chez eux par réseau virtuel (VPN).

## Les différents acteurs

Identifier les différents acteurs suppose une bonne connaissance des usages des utilisateurs. Par « utilisateur », on entend toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux moyens informatiques et de communication électronique, quel que soit son statut.

La décentralisation fait que les collectivités gèrent de plus en plus de tâches ; ce qui les oblige à faire appel à des prestataires privés extérieurs. Le personnel des prestataires de services de la collectivité sera considéré comme utilisateur du système d'information. Le système d'information doit donc gérer de nombreux métiers différents (le système doit pouvoir gérer les agents administratifs dans l'enceinte de la collectivité mais aussi les personnes rattachées en tant que sous-traitants), avec pour chacun un langage spécifique et donc un empilement de logiciels spécialisés interopérables.

## Données personnelles

Dès le moment où le système d'information de la collectivité collecte et traite des données personnelles (noms, prénoms des agents par exemple), des contraintes liées à la loi Informatique et libertés s'appliquent.

Par données nominatives, il y a lieu d'entendre les informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent, telles que par exemple les adresses électroniques.

Cette loi ne protège pas l'agent qui utiliserait de manière abusive à des fins personnelles les outils informatiques qui sont mis à sa disposition.

Les utilisateurs devront être informés de la légitimité du traitement des données personnelles, que ce soit au niveau de la concertation collective ou par le biais de l'information individuelle et de l'adhésion à la charte.

Les principes de proportionnalité (action proportionnée aux buts visés), de transparence (information préalable des acteurs avant tout contrôle) et de conservation limitée des données

# Préserver le système d'information, assurer la qualité, le bon fonctionnement et la continuité du service public, dans le respect des droits et libertés de chacun.

qualifie le comportement abusif d'abus de confiance. Le 19 mai 2004, la Cour de cassation a considéré que le salarié se rendait coupable d'abus de confiance dans l'utilisation de l'ordinateur professionnel et de la connexion Internet. La situation était particulière puisque le salarié surfait très longtemps sur des sites pornographiques et avait même créé un site pornographique dont l'adresse contenait le nom de l'entreprise. On est donc ici dans un cas extrême. La casuistique sera de rigueur puisque le juge apprécie « in concreto » et donc souverainement l'abus.

La cybersurveillance des agents publics se teinte d'une autre dimension liée au statut de la fonction publique. L'utilisation inappropriée d'un agent public du système d'information mis à sa disposition peut justifier une sanction disciplinaire. Dans ce cadre, le Conseil d'Etat, le 15 octobre 2003, vient sanctionner le comportement d'un adjoint technique qui avait utilisé l'adresse

d'information de la collectivité.

L'objet rappellera le nécessaire respect des règles visant à assurer la sécurité, le bon fonctionnement du service, la performance des traitements, la préservation des données confidentielles et le respect des dispositions légales et réglementaires qui s'imposent.

## Définir l'étendue du système d'information

Il est important dès le départ d'identifier tous les outils de communication électronique dépendant du système d'information. Le système d'information d'une collectivité contient à la fois l'ensemble des ordinateurs fixes et portables, ainsi que les téléphones mobiles, en passant par des assistants numériques personnels ou PDA. L'évolution des mobiles en fait des terminaux communicants pouvant donner accès au système d'information de la collectivité.

Les logiciels contenus mais aussi les protocoles de communication font partie

personnelles seront observés. Toutes les créations de fichiers comprenant ce type d'informations, y compris lorsqu'elles résultent de croisement, d'interconnexion de fichiers préexistants, doit impérativement faire l'objet d'une déclaration et/ou demande d'avis préalable à la Commission nationale Informatique et libertés (CNIL).

En conséquence, tout « utilisateur » souhaitant procéder à un tel traitement devra en informer préalablement le service de la collectivité qui prendra les mesures nécessaires au respect des dispositions légales.

Par ailleurs, conformément aux dispositions de la loi Informatique, fichiers et libertés n°78-17 du 6 janvier 1978 modifiée, chaque « utilisateur » dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation du système d'information. Ce droit s'exerce en principe auprès du service informatique de la collectivité ou des ressources humaines.

## Rôle pivot de l'administrateur système

Maillon essentiel de la rédaction de la charte, il est le principal exécutant de la charte et veille au respect par chacun de la bonne utilisation du système d'information.

La rédaction tiendra donc compte des conseils techniques de l'administrateur système, à savoir en général le responsable du service informatique désigné en tant qu' « administrateur » du système d'information. Il sera également dans quelques cas le garant de la mise en conformité du système d'information avec les dispositions légales, et effectuera toute formalité ou déclaration, en particulier celles issues de la loi Informatique et libertés du 6 janvier 1978 (déclaration et gestion des fichiers contenant des données personnelles) et de la loi du 10 juillet 1991 sur le secret des correspondances (veille sur le respect du secret des correspondances). Ainsi, il serait intéressant d'envisager le statut de correspondant CNIL (déjà prévu dans la loi d'août 2004 pour les entreprises privées) pour l'administrateur réseau afin de garantir une communication efficace entre la CNIL et la collectivité.

L'administrateur pourra être enfin le déclencheur de l'alerte, en prévoyant notamment les données informatiques à conserver et la traçabilité à mettre en place en vue de garantir la politique de sécurité de la collectivité. La direction générale des services sera immédiatement saisie lors de la détection d'un abus.

## Citoyenneté numérique

### Pédagogie du changement

La charte devra être complétée par des annexes technique et juridique qui définissent respectivement les principales règles pratiques et juridiques de mise en œuvre des règles permanentes et générales figurant dans la charte. Le maniement des notions informatiques

## Assurer à la charte la plus grande diffusion et l'associer à des actions de sensibilisation des utilisateurs permet de lui assurer dans les faits une efficacité maximale.

implique que les utilisateurs s'en imprègnent. Ils doivent se familiariser progressivement avec elles. Des séances de formation interne sont un préalable intéressant.

### Utilisation privée, utilisation professionnelle

La règle étant bien entendu l'utilisation professionnelle, l'exception de l'utilisation privée n'en est pas moins autorisée à condition qu'elle soit non lucrative et limitée tant dans sa fréquence que dans sa durée.

Il faudra donc envisager la création d'îlots de vie privée à l'intérieur de l'utilisation professionnelle ; l'agent stockera ses données à caractère privé (messages, lettres, carnets d'adresses, photos, vidéos, etc.) dans un répertoire de données nommé « Privé » ou « Personnel ».

La localisation de ce répertoire pourra se situer sur le disque dur personnel de l'utilisateur (partie généralement appelée C:\) et ne sera donc pas inclus dans les sauvegardes. Ainsi, la sauvegarde régulière incombera à l'agent, sous sa seule responsabilité.

### Protection de la vie privée

Respecter la vie privée des utilisateurs, c'est d'abord les informer du nécessaire respect des dispositions sur la gestion des données nominatives informatisées de loi informatique et libertés n° 78-17 du 6 janvier 1978 modifiée en août 2004 dite Informatique et libertés.

Chaque utilisateur a par ailleurs droit au respect de sa vie privée. Il sera de bon ton de définir dès lors le périmètre de la vie privée de l'utilisateur en précisant ce qu'il est ou non possible de faire à titre personnel en rappelant qu'il n'est pas possible d'interdire totalement l'usage à titre personnel des Courriels et autres moyens informatiques, et

ce notamment au vu de la dernière jurisprudence en la matière.

### Gestion des rôles

La dématérialisation de l'ensemble des données de la collectivité implique une sécurisation accrue du système.

La collectivité octroie un droit d'accès à l'utilisateur. Ce droit d'accès est personnel et incessible. Les conditions d'accès au réseau, la gestion des mots

de passe, les conditions de protection de certains fichiers, la sécurité liée aux PC portables sont précisées dans la charte. Ainsi, des niveaux d'accès des utilisateurs sont définis en fonction de leur profil, établi selon les critères propres au statut de chacun. C'est ce que l'on appelle la gestion des rôles : un responsable de collectivité aura ainsi la possibilité d'utiliser la plupart des fonctionnalités du système, alors qu'un agent technique ne pourra que consulter son emploi du temps, par exemple. Cette gestion permet ainsi de gérer la ressource en amont.

### Placer l'utilisateur au centre

L'utilisateur est un maillon essentiel de la sécurité du système et la condition sine qua non de l'application de la charte. Il doit être au centre de la réflexion lors des différents moments de la vie de la charte. Il sera donc informé « ab initio » sur la volonté de la direction de mettre en place une charte et sur les raisons d'être de ces nouvelles règles.

Bien souvent, ce type de guide de bonne conduite rassure les agents car ils ne connaissent pas en général l'étendue de leurs droits envers un système d'information. Cela permet de les responsabiliser sur l'utilisation du système et de les faire contribuer à son bon fonctionnement par leurs actions de détection des anomalies techniques, la mise à jour de leurs logiciels antivirus et par le classement des fichiers publics et privés sur des répertoires différents, allégeant ainsi les sauvegardes quotidiennes des données du système d'information. L'utilisateur devra en cas d'anomalie sur le système stopper toute transaction et prévenir immédiatement l'administrateur.

Dernier élément concernant l'utilisateur, qui est 9 fois sur 10 un agent public,

il devra respecter son obligation de confidentialité et de discrétion à l'égard des documents confidentiels auxquels il pourrait avoir accès.

## Gestion technique

### Surveillance fondée

Un système d'information, pour rester performant, doit pouvoir être audité régulièrement à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus. L'administrateur fera les opérations techniques requises en vue du bon fonctionnement du système.

### Sécurité antivirale

Les postes de travail sont en général tous équipés d'un logiciel antivirus conforme aux règles édictées par la direction des services. Aussi, tout élément, même s'il est destiné à un agent, s'il est bloquant ou s'il présente une difficulté technique, pourra être mis en quarantaine pour désinfection, voire destruction au cas où la réparation s'avèrerait impossible.

### Gestion des courriels

Les agents disposent d'une boîte aux lettres nominative qui leur permet de recevoir et d'émettre des messages électroniques ou « mails ». Considéré comme un acte public, le message électronique sera considéré comme un acte professionnel. Une exception existe cependant, lorsque l'agent insère la mention « personnel » ou « privé » dans la zone « objet » du message.

Les formats, type et taille des messages pourront être limités. Le contenu du message ne devra pas être illicite et sera rédigé par l'utilisateur en tenant compte de la possible valeur juridique en tant que preuve (ad probationem) et même depuis peu (loi pour la confiance dans l'économie numérique et ordonnance du 17 juin 2005) en tant que validité (ad validitatem) de son Courrier émis. Le message électronique pourra engager la collectivité sous certaines conditions et des contrats pourraient être formés de manière inopinée. La vigilance sera donc de rigueur.

## Téléchargement et propriété intellectuelle

La protection est de rigueur face au téléchargement de logiciels ou d'œuvres sans autorisation pouvant engager la responsabilité de la collectivité. La charte prévoit en général toutes les actions prohibées qui vont avec le développement du « P2P » (Kazaa ou autre eMule) sur tous types de contenus de plus en plus nombreux.

L'utilisateur respectera les droits de propriété intellectuelle en utilisant par exemple les logiciels dans les conditions des licences souscrites. Ce qui doit normalement lui suggérer de ne pas utiliser sa licence professionnelle pour utiliser le logiciel sur d'autres postes à l'extérieur du système d'information.

### Forums de discussion et blogs

La participation à des blogs ou à des forums de discussion peut engager la responsabilité de la collectivité. Aussi, l'utilisateur veillera à disposer des autorisations internes avant de s'exprimer au nom de la collectivité.

### Evolution de la charte

La collectivité devra mettre en place une veille et un suivi des évolutions de la charte. Par exemple, en prenant connaissance des nouvelles positions et principes de la CNIL, en évaluant les nouveaux besoins techniques des agents, et en suivant la jurisprudence. L'évolution des techniques de sécurité informatique (géolocalisation ou biométrie par exemple) impactera le contenu futur de la charte.

### Accessibilité de la charte

La charte sera mise en ligne en général sur le site Intranet de la collectivité et sera réputée, à compter de cette date, avoir été portée à la connaissance de l'ensemble des utilisateurs. Il conviendra d'établir les moyens de diffusion de la charte afin que celle-ci soit le plus largement connue.

Compte tenu de l'absence de valeur juridique contraignante de ce type de charte, la prise d'effectivité sera subordonnée à une prise de décision de la collectivité (décision de l'assemblée délibérante ou d'une commission paritaire) ou insertion de la charte dans un règlement intérieur.

## Ressources pratiques

Panorama des évolutions des systèmes d'information des collectivités locales

[http://www.01net.com/article/237357\\_a.html](http://www.01net.com/article/237357_a.html)

Le changement des habitudes des administrations avec le numérique

<http://www.admiroutes.asso.fr/mission/rapport/rapport.htm>

Analyse des tenants et aboutissants de la mise en place d'un intranet au sein d'une collectivité

[http://www.ardesi.asso.fr/admin/upload/fichier/213-presentation\\_wsinteractive.ppt](http://www.ardesi.asso.fr/admin/upload/fichier/213-presentation_wsinteractive.ppt)

Modèle de charte relative à l'utilisation d'un système d'information

[http://www.legalis.net/legalnet/contrats/sys\\_information.htm](http://www.legalis.net/legalnet/contrats/sys_information.htm)

Exemple de la charte du Département de mathématiques d'Orsay

<http://www.math.u-psud.fr/infos/Charte-web.html>

Exemple de la charte déontologique de RENATER

[http://www.unicaen.fr/crisi/legislation/legis\\_reseau.htm](http://www.unicaen.fr/crisi/legislation/legis_reseau.htm)

Exemple de la charte de l'université Bordeaux 2

[http://www.u-bordeaux2.fr/intranet/public/charte/charte\\_ub2\\_personnel\\_cri.pdf](http://www.u-bordeaux2.fr/intranet/public/charte/charte_ub2_personnel_cri.pdf)

Exemples de clauses de charte dans l'éducation

<http://www.educnet.education.fr/juri/juriscol/fiche32.htm>

La vie privée au travail

[http://lexinter.net/JP/vie\\_privée\\_au\\_travail.htm](http://lexinter.net/JP/vie_privée_au_travail.htm)

La cybersurveillance des salariés

[http://www.caprioli-avocats.com/pages/publications/edocs/donnees\\_perso/edocs\\_donneesperso\\_cybersurveillance.htm](http://www.caprioli-avocats.com/pages/publications/edocs/donnees_perso/edocs_donneesperso_cybersurveillance.htm)

La jurisprudence sur la cybersurveillance

[http://www.legalis.net/jurisprudence.php3?id\\_rubrique=14](http://www.legalis.net/jurisprudence.php3?id_rubrique=14)

L'utilisation abusive des téléphones professionnels

<http://sullimano.tooblog.fr/?2005/07/25/14-le-mobile-de-lentreprise-cest-bien-en-abuser-ca-craint>

L'arrêt Nikon

<http://www.men.minefi.gouv.fr/webmen/revuedeweb/cybersurveillance.html>

La jurisprudence après l'arrêt Nikon

- <http://www.foruminternet.org/actualites/lire.phtml?id=787>  
- <http://www.net-iris.com/veille-juridique/doctrine.php?document=354>

La dernière position de la Cour de cassation sur la cybersurveillance

[http://www.legalis.net/archives.php3?id\\_rubrique=155](http://www.legalis.net/archives.php3?id_rubrique=155)