

Citation : Caprioli & Associés, Démarche pour la mise en place d'une charte "informatique et communications électroniques" dans les collectivités territoriales, <http://www.caprioli-avocats.com>

Date de la mise à jour : juin 2004

### Démarche pour la mise en place d'une charte " informatique et communications électroniques " dans les collectivités territoriales

Eric A. Caprioli  
contact@caprioli-avocats.com

---

#### Plan

#### A) L'ENVIRONNEMENT JURIDIQUE

#### B) ELABORATION ET MISE EN PLACE DE LA CHARTE

1. Prise en compte de l'environnement juridique existant
2. Examen des objectifs et des besoins du client
3. Exposé des contraintes
4. Etablissement d'un plan d'action
5. Rédaction d'un projet de charte et de la procédure à suivre
6. Discussion et négociation du texte
7. Suivi de la procédure jusqu'à l'entrée en vigueur

#### Notes

---

A l'heure de l'Internet, les personnes publiques (administrations d'Etat et collectivités locales) et privées, exposées à des attaques extérieures, s'orientent vers la mise en place de mesures de sécurité destinées à prévenir les risques, voire à repérer l'origine des problèmes. Dans cette optique protectionniste, les employeurs publics peuvent être incités à mettre en place des mesures de contrôle des agents relatives à l'utilisation des moyens informatiques (poste de travail) et des communications électroniques (technologie de l'information et télécoms) au sens de l'article 1er du projet de loi pour la confiance dans l'économie numérique [1].

Par un arrêt du 15 octobre 2003 [2], le Conseil d'Etat a confirmé la décision de la Cour administrative d'appel de Paris rejetant le recours d'un adjoint technique de recherche contre une sanction disciplinaire prise suite à l'utilisation abusive d'une adresse électronique professionnelle. L'agent avait utilisé son adresse électronique professionnelle puis celle de son directeur de laboratoire, à l'insu de ce dernier, pour communiquer en tant qu'adhérent sur le site de l'Association pour l'Unification du Christianisme Mondial, plus connue sous le nom de secte Moon. Le Conseil d'Etat a considéré que le simple fait d'avoir utilisé une adresse électronique professionnelle, qui plus est celle d'un autre agent, à des fins personnelles et que cette adresse apparaisse comme émanant d'un " membre " sur un site religieux " *constituaient un manquement au principe de laïcité et à l'obligation de neutralité*[3] *qui s'imposent à tout agent public*". Cette affaire, même si elle reste malgré tout fondée sur le respect traditionnel de droits et de devoirs par les fonctionnaires dans le cadre de leur mission [4], attire l'attention sur la nécessité d'un contrôle de l'activité des agents par leur supérieur pour éviter que la simple utilisation de moyens informatiques ne se retourne contre l'agent ou contre l'administration elle-même. Dans le cadre d'une utilisation abusive de ces moyens par l'agent, est mise en exergue la question de la responsabilité. Il convient de rappeler à cet égard qu'il existe un risque de condamnation pénale qui pèse non seulement sur la collectivité territoriale " *pour les infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de délégation de service public* " [5] mais aussi sur le chef de service sous certaines conditions posées à l'article 121-3 du code pénal [6]. Ainsi, il convient de responsabiliser les agents sur les conséquences de leurs actes non seulement pour eux [7] mais aussi pour la collectivité. Concernant la responsabilité civile des agents, c'est la distinction traditionnelle entre faute de service et faute personnelle qui s'applique. Ainsi les agents ne peuvent voir leur responsabilité civile engagée du fait des actes qui sont accomplis dans le cadre de leur mission [8], même si de telles fautes peuvent être sanctionnées disciplinairement [9]. Encore faut-il qu'une telle sanction soit proportionnelle à la gravité de la faute commise. De plus, la procédure de mise en œuvre de telles sanctions est assez complexe (saisine de la commission administrative paritaire qui siège en conseil de discipline, communication du dossier...) [10]. En tout état de cause, la collectivité doit se prémunir contre ce genre d'agissements à la fois par l'élaboration d'une politique de sécurité et par la mise en place d'un contrôle préventif de l'usage des outils de communication mis à la disposition des agents.

Mais un tel contrôle peut s'avérer parfois en contradiction avec les règles relatives au respect de la vie privée et à la protection de données personnelles issues de la loi du 6 janvier 1978, aux règles de droit public, voire au droit du travail [11] (ex : le personnel des Etablissements Publics Industriels et Commerciaux (EPIC), à l'exception du chef d'établissement et du comptable public, est soumis au régime de droit privé [12] ou encore possibilité pour certains agents non titulaires bénéficiant d'un contrat à durée indéterminée de demander que ce contrat avec la collectivité soit soumis aux dispositions du code du travail [13]), ainsi que d'un certain nombre de directives européennes qui, faute d'être intégrées au droit national, sont parfois susceptibles d'une application directe en droit interne [14]. C'est pourquoi, en cette matière, il faut que les règles du jeu soient fixées, que les objectifs de sécurité de la personne publique et de ses agents, de continuité du service public soient énoncés et enfin que les activités permises et leurs limites soient établies. La charte " *informatique et des communications électroniques* " (ci-après la charte informatique), de nature contractuelle, est l'instrument juridique qu'il convient de mettre en place. L'adhésion des agents et leur participation au processus d'élaboration est en outre nécessaire au bon déroulement du projet.

Nous envisagerons tour à tour, le cadre juridique général au sein duquel la charte " informatique " prend place (A) et l'élaboration et la mise en place de la charte (B).

## A) L'ENVIRONNEMENT JURIDIQUE

La collectivité doit respecter un certain nombre d'obligations légales en matière de données nominatives (ex : acte réglementaire pris après avis motivé de la CNIL pour les traitements informatisés de données personnelles, confidentialité et sécurité de tels traitements, droits accordés aux personnes concernées par le traitement). En cas de manquement, le responsable du traitement s'expose à de sévères sanctions pénales (ex : les articles 226-16 à 226-24 du Code pénal prévoient jusqu'à 5 ans d'emprisonnement et 300.000 € d'amende). Il en va de même pour les données personnelles diffusées par un Intranet. Ainsi les annuaires, les forums de discussion ou bien les cookies peuvent comporter de telles données et être donc soumis aux mêmes règles juridiques.

Armé de tels outils puissants et face à une utilisation parfois abusive par les agents des nouvelles technologies mises à leur disposition, l'employeur public entend exercer ses prérogatives qui découlent soit du régime statutaire et réglementaire de la fonction publique [15], soit du contrat liant la collectivité et ses agents soit encore de règles concernant les droits et devoirs des membres de la fonction publique [16]. Malgré cette légitimité apparente du contrôle des activités des agents, force est de constater que l'employeur public devra composer avec les règles applicables en matière de secret des correspondances. Cela souligne bien le paradoxe existant en matière de Nouvelles Technologies de l'Information et de la Communication (NTIC) entre d'un côté, un principe de responsabilité du chef de service du fait des actes accomplis par ses agents dans l'exécution du service et, par conséquent, la nécessité d'un contrôle du chef sur les activités de ses agents, et, de l'autre, l'obligation du chef de service de respecter les libertés individuelles de l'agent.

On peut considérer que le contrôle exercé par l'employeur public est conditionnel :

- il ne saurait porter atteinte à la vie privée et à l'image des agents (article 9 du Code civil [17]). Le respect de la vie privée est aussi énoncé à l'alinéa 1er de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ainsi rédigé : " *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ". De plus, le principe de proportionnalité posé par l'article L.120-2 du Code du travail 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. " est appliqué par les juridictions administratives [18].

- il doit faire l'objet d'une information préalable des agents (et des organes représentatifs). Selon la loi 78-17 du 6 janvier 1978 [19] relative à l'informatique, aux fichiers et aux libertés, tout traitement automatisé d'informations nominatives opéré pour le compte d'une collectivité territoriale doit faire l'objet, s'il n'a pas été autorisé par la loi, d'un acte réglementaire pris après avis motivé de la CNIL et si cet avis est défavorable, la collectivité pourra passer outre mais " *en vertu d'une décision de son organe délibérant approuvée par décret pris sur avis conforme du Conseil d'Etat* ". De plus, elle interdit que les données soient collectées par un moyen frauduleux, déloyal ou illicite [20] et impose une obligation d'information des personnes concernées, relative à la destination des informations recueillies ainsi qu'à l'existence d'un droit de rectification pour les données personnelles les concernant [21]. En outre, l'article 12 du décret n°82-452 du 28 mai 1982 relatif aux comités techniques paritaires [22] impose une information et une consultation préalable de ces comités techniques paritaires concernant " *les questions et les projets de textes relatifs : [...] 3° Aux programmes de modernisation des méthodes et techniques de travail à leur incidence sur la situation du personnel* ". La charte ayant une incidence sur les méthodes de travail des agents, les dispositions de ce décret s'appliqueront donc pleinement.

- il doit être justifié par un intérêt légitime (tel que prévenir la fraude, assurer la sécurité) et être proportionnel au but recherché. Comme l'a énoncé la CNIL, le contrôle ne peut avoir pour seul but de contrôler l'activité professionnelle des agents.

La charte fournit les moyens juridiques aux collectivités territoriales pour encadrer l'utilisation de l'informatique et des communications électroniques. Les règles adoptées ont pour objectif de prévenir les risques juridiques, économiques et techniques de la collectivité. Touchant à l'organisation des services, cette charte devra être

adoptée après consultation du comité technique paritaire. De plus, pour recueillir une adhésion forte et donc une efficacité renforcée de la charte, il faudra accompagner la diffusion de ce document d'une démarche pédagogique auprès des personnels concernés. En effet, " *la sécurité ne s'impose pas, elle s'inculque* " [23] et il faut d'abord informer les utilisateurs des risques et des failles de ces moyens de communication et les responsabiliser. La charte permet aux collectivités d'assurer la sécurité de leurs systèmes d'information et de contrôler l'usage que les agents font des outils informatiques mis à leur disposition. La sensibilisation et l'information des agents constituent, à notre avis, des éléments clés, sans doute, plus importants que les sanctions associées aux manquements aux règles.

## **B) Elaboration et mise en place de la charte**

La rédaction d'une charte d'utilisation des moyens informatiques et des réseaux (y compris l'intranet) au sein de la collectivité peut s'avérer décisive pour établir les règles de droit et d'usage, de déontologie et de manière plus générale de sécurité relatives à l'utilisation des ressources informatiques.

Mais l'élaboration d'une telle charte dans le cadre des collectivités territoriales présente des spécificités par rapport au droit privé, notamment en ce qui concerne sa valeur juridique. En effet, il n'existe pas, dans les collectivités territoriales, d'équivalent du règlement intérieur pour les entreprises privées auquel une charte pourrait se rattacher. Ainsi, l'efficacité d'une telle charte en droit public est plus limitée qu'en droit privé. Il n'en demeure pas moins que la fonction publique territoriale regroupe essentiellement deux types d'agents : les agents contractuels et les agents titulaires.

Pour les agents contractuels, il sera aisé d'intégrer la charte au contrat de travail et donc d'en faire un document contractuel à part entière susceptible d'aboutir à des sanctions en cas de violation de ses dispositions. Pour les agents titulaires, la question se pose en des termes différents. En effet, l'une des spécificités du régime juridique des fonctionnaires tient à leur situation déterminée de façon légale et réglementaire. Ainsi, les modifications du statut des agents publics titulaires ou même stagiaires ne peuvent intervenir que par voie réglementaire ou législative. Malgré tout, l'administration ne dispose pas d'un pouvoir arbitraire en la matière puisque, depuis 1946, la puissance publique a été amenée peu à peu à examiner et discuter avec ses agents des différents éléments de leurs statuts et de leurs conditions de travail. Elle doit notamment consulter le comité technique paritaire pour tout ce qui touche à l'organisation et aux règles générales de fonctionnement du service concerné (V. infra le point n°7). De plus, la charte, même si elle n'aura pas nécessairement la même efficacité que dans l'entreprise privée, aura pour fonction d'informer et de sensibiliser les agents sur les risques que peuvent générer une mauvaise utilisation ou une utilisation imprudente des nouveaux moyens de communication. Adopter une telle charte représente donc un réel atout pour les collectivités.

A cette fin, la démarche juridique à emprunter s'effectuera en trois phases : cadrage, analyse et rédaction, négociation et mise en œuvre. Elle doit suivre les points mentionnés ci-après.

### **1. Prise en compte de l'environnement juridique existant**

Tous les documents pertinents doivent être intégrés dans l'analyse, par exemple : la Charte en vigueur ou en projet, la politique de sécurité (si elle existe, ou la politique de sécurité informatique), les notes de service, les recommandations sectorielles, syndicales ou tout autre document permettant de connaître l'environnement juridique de la collectivité concernée.

### **2. Examen des objectifs et des besoins du client**

La collectivité devra établir un inventaire détaillé des moyens fournis au personnel et des moyens de contrôle et de surveillance (par exemple, logiciels, bases de données, filtrage) ainsi que des interdictions et limites d'utilisation qu'elle envisage. La charte devra contenir des dispositions qui fixeront les règles de bonne conduite que les agents utilisateurs s'engagent à respecter au sein de la collectivité concernant les moyens informatiques. Dans ce cadre, il faudra déterminer une séparation entre les sphères professionnelle et privée des agents. Par exemple, la charte pourra préciser que les utilisateurs disposent d'une adresse électronique professionnelle déterminée. Leur attention sera alors attirée sur le fait que leur messagerie professionnelle doit servir exclusivement pour leurs activités professionnelles. Il conviendra néanmoins de déterminer dans la charte l'utilisation raisonnable des réseaux à titre personnel.

### **3. Exposé des contraintes**

Le projet de charte est complexe avec d'une part, une très forte interaction dans divers domaines juridiques (social, pénal, droits et libertés fondamentales) et d'autre part, avec la mise en relation de plusieurs directions de l'organisme (sécurité des systèmes d'information, informatique, communication, juridique, ressources humaines, services usagers, ...) nécessitant une concertation poussée au sein de la collectivité. Par conséquent,

la mise en œuvre du projet doit être guidée par les principes de transparence et de proportionnalité. Un certain nombre de précisions doivent être fournies (définition du contenu de la charte et de l'encadrement juridique des utilisations) ainsi que des règles et des sanctions en cas de violation.

La charte doit traiter des moyens informatiques (applicatifs et matériels) et de l'utilisation des technologies de l'information et de la communication (connexions et accès aux réseaux et bases de données de l'entité concernée). Un accent particulier devra être mis sur la sensibilisation du personnel. Cet aspect est d'autant plus important que l'on se situe en matière de fonction publique. En effet, comme l'instauration de sanctions ne pourra pas être effectuée aussi facilement que dans les entreprises privées, du fait du caractère principalement statutaire et réglementaire - et donc difficilement modifiable - du régime des agents (V. supra le point B, la distinction des régimes contractuel et statutaire), le moyen le plus efficace de faire respecter cette charte est de la communiquer et l'expliquer en termes clairs aux agents. La direction générale devra décider du moment où la participation du personnel sera requise : dès le lancement du projet ou seulement pour avis ?

#### **4. Etablissement d'un plan d'action**

Ce document doit être piloté par un chef de projet. Il doit être suffisamment précis, détaillé étape par étape en mentionnant toutes les actions à mener, les personnes responsables et ce jusqu'à la fin du projet. Des dates pour la mise en place de chaque étape du projet devront être fixées.

#### **5. Rédaction d'un projet de charte et de la procédure à suivre**

Pour aboutir à une plus grande efficacité de la charte, ses objectifs devront être définis au regard de l'analyse des contraintes juridiques de la collectivité. La procédure concerne non seulement les représentants du personnel (ex : Comité technique paritaire) et les agents, mais aussi les déclarations et communications externes (CNIL pour la demande d'avis motivé,...). La charte devra déterminer et préciser certaines rubriques et les décliner en fonction des besoins spécifiques de l'entité : Préambule/Généralités ; Objet (objectifs poursuivis, principes, moyens) ; Respect des libertés et des droits fondamentaux des agents ; Usages autorisés, limités ou interdits (professionnels, privés) ; Contrôle/surveillance ; Droits des agents et des représentants du personnel ; Modalités d'application (procédure d'entrée en vigueur et sanctions).

#### **6. Discussion et négociation du texte**

Cette étape débutera avec une mise au point et une finalisation des documents par l'équipe chargée du projet en concertation avec les chefs de service et les représentants du personnel, ce qui permettra ensuite d'enclencher la procédure d'information et de consultation des agents suivant les modalités déterminées pendant les étapes antérieures.

#### **7. Suivi de la procédure jusqu'à l'entrée en vigueur**

Tout au long de la procédure, la collectivité a l'obligation de consulter les représentants du personnel [24] ainsi que le comité technique paritaire et de communiquer les documents de la charte. Concernant les comités techniques paritaires, ceux-ci n'ont que des pouvoirs exclusivement consultatifs et la décision revient toujours, en dernier ressort, à l'autorité hiérarchiquement compétente. Néanmoins, quand leur consultation est obligatoire, notamment pour les chartes informatiques car elles touchent à l'organisation du service et ont une incidence sur les conditions de travail des agents, son omission ou encore une irrégularité substantielle dans cette procédure de consultation entache d'illégalité l'acte final, c'est-à-dire la charte.

Le recours à des nouvelles technologies de communication et d'information s'impose à toutes les entreprises qu'elles soient privées ou publiques. Cette utilisation ne saurait se développer sans la prise en compte des cadres juridiques qui permettent de garantir le respect des libertés fondamentales (protection des données personnelles, droits des agents). A cet égard, la rédaction de chartes "informatiques" peut réaliser la nécessaire conciliation entre les obligations auxquelles sont tenus les employeurs publics vis-à-vis de leurs agents (en terme de respect des libertés individuelles, par exemple) et les obligations qui leur incombent en ce qui concerne le contrôle de leurs activités et la sécurité de leur service.

#### **Notes**

[1] V. site de l'Assemblée Nationale : <http://www.assemblee-nat.fr/12/projets/pl0528.asp> sous réserve des modifications effectuées au projet de loi par la suite.

[2] CE, 15 octobre 2003, Jean-Philippe O. c/ Ministère de l'éducation nationale et de la recherche, req. n°244428, Recueil Lebon 2003 (à paraître).

[3] V. sur cette obligation : René Chapus, Droit administratif général, Tome 2, Montchrestien, 15ème éd., 2001, p. 245 et s.

[4] En effet, il faut mesurer la portée réelle de cet arrêt. Le Conseil d'état s'appuie uniquement sur le principe de laïcité et l'obligation de neutralité que doit respecter le fonctionnaire pour justifier la sanction disciplinaire dont ce dernier a fait l'objet. Reste à savoir, si dans le cadre d'une utilisation autre de l'adresse électronique par le fonctionnaire, par exemple sur un site n'ayant pas de caractère religieux, la solution aurait été la même.

[5] V. l'alinéa 2 de l'article 121-2 du code pénal.

[6] En effet, l'alinéa 4 de l'article 121-3 du code pénal dispose : " *Dans le cas prévu par l'alinéa qui précède, les personnes physiques qui n'ont pas causé directement le dommage, mais qui ont créé ou contribué à créer la situation qui a permis la réalisation du dommage ou qui n'ont pas pris les mesures permettant de l'éviter, sont responsables pénalement s'il est établi qu'elles ont, soit violé de façon manifestement délibérée une obligation particulière de prudence ou de sécurité prévue par la loi ou le règlement, soit commis une faute caractérisée et qui exposait autrui à un risque d'une particulière gravité qu'elles ne pouvaient ignorer.* "

[7] L'alinéa 3 de l'article 121-2 du code pénal dispose en effet : " *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.* "

[8] Et cela va même plus loin car la jurisprudence a tendance à avoir une conception assez extensive de la faute de service au point d'admettre qu'une faute non dépourvue de tout lien avec le service permet d'engager la responsabilité de l'administration (à charge pour elle de se retourner en suite contre l'agent) : V. André de Laubadère et Yves Gaudemet, *Traité de droit administratif*, Tome 5, La fonction publique, L.G.D.J., 12ème éd., 2000, p.158.

[9] V. P. Bandet, *Le droit disciplinaire de la fonction publique territoriale*, Ed. Le Moniteur, 1 990 et E. Peuchot, *Le régime disciplinaire applicable aux fonctionnaires territoriaux*, Les Petites Affiches, 6 mars 1989, p. 10.

[10] Concernant le régime disciplinaire, v. René Chapus, *Droit administratif général*, op. cit., p. 330 et s.

[11] V. Eric Caprioli, *La cybersurveillance des salariés, Du droit à la pratique des chartes informatiques*, Petites affiches, 2004, (à paraître).

[12] Jurisprudence constante depuis l'arrêt du Conseil d'état, 8 mars 1957, Jalenques de Labeau, J.C.P. 1957, II, 9987, note Dufau.

[13] Loi n°2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations (article 35), J.O. 13 avril 2000, p.5646

[14] C'est le cas notamment pour la directive n° 95/46/CE du Parlement 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 (J.O.C.E. du 23 novembre 1995, L. 281/31) et pour la directive n° 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (J.O.C.E. du 31 juillet 2002, L. 201/37).

[15] Loi n°84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale modifiée, J.O. 27 janvier 1984, p. 441.

[16] V. notamment la loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires dite " loi Le Pors " modifiée, J.O. 14 juillet 1983, p. 2174.

[17] A cet égard, v. CE, 30 décembre 2002, M. Marcel A. et Syndicat "Lutte pénitentiaire" (SLP), req. n° 224721, où le Conseil d'état vise expressément l'article 9 du code civil.

[18] V. par ex. CE, référé, 25 juillet 2003, Ministre de la jeunesse, de l'éducation et de la recherche c/ Syndicat national unifié des directeurs, instituteurs et professeurs des écoles de l'enseignement public -Force ouvrière (SNUDI-FO), req. n°258677.

[19] Article 15 de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O. 7 janvier 1978, p. 227.

[20] V. l'article 25 de la loi précitée et l'article 226-18 du code pénal.

[21] Article 27 de la loi précitée et article 226-18 du code pénal.

[22] Décret en Conseil d'Etat 82-452 du 28 mai 1982, J.O. 30 mai 1982, p. 1735.

[23] V. sur le sujet Anne Cantéro, *Les collectivités locales et la sécurité informatique*, La Gazette des communes n° 34/1708 du 15 septembre 2003, p. 70.

[24] En effet, selon l'article 9 de la loi n°83-634 du 13 juillet 1983 précitée : " Les fonctionnaires participent, par l'intermédiaire de leurs délégués siégeant dans des organismes consultatifs, à l'organisation et au fonctionnement des services publics, à l'élaboration des règles statutaires et à l'examen des décisions individuelles relatives à leur carrière."