REGLEMENT D'UTILISATION DE L'INFORMATIQUE AU CETE MEDITERRANEE

Vu l'avis du CTPS du 14/01/2004
Vu la demande de conseil CNIL N°04003855 en date du 9/04/2004

L'introduction des technologies de l'information et de la communication (TIC) transforme les modes de traitement, d'utilisation et de diffusion de l'information professionnelle et de l'information privée. L'objet du présent règlement est donc de définir les conditions de leurs usages (messagerie, internet, données) dans le cadre du dispositif législatif et réglementaire et des préconisations de la CNIL relative à la cybersurveillance sur les lieux de travail.

1) Objet du règlement

Le CETE met à disposition de chaque agent dans le cadre de ses fonctions un ordinateur doté des logiciels et des connexions réseaux selon la politique informatique définie par le ministère et mis en œuvre en interne selon notre plan d'informatisation.

Chaque agent est responsable de l'ordinateur mis à sa disposition et des données qu'il y stocke .

De façon générale, un agent ne peut pas accéder au poste d'un autre agent sans son autorisation sauf dans les cas définis au présent règlement ou dans les cas prévus par l'organisation spécifique du service.

Le présent règlement a pour objet de définir les droits et obligations de l'administration et des agents (y compris vacataires et stagiaires) dans l'usage des postes informatiques du CETE et des services associés (messagerie, internet, intranet, …).

Le présent règlement ne se substitue pas aux textes réglementaires ou législatifs, ni aux directives interministérielles ou ministérielles ; il les décline dans le cadre spécifique du CETE.

Le présent règlement est remis à tous les utilisateurs de l'informatique du CETE.

2) Rappels réglementaires

Le développement des TIC a fait évoluer le droit, il est donc important de rappeler le cadre législatif et réglementaire applicable.

* La protection des personnes, visée par la Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui réglemente les traitements automatisés des informations nominatives.

> La loi impose de procéder à une déclaration auprès de la CNIL avant toute mise en oeuvre de traitement de ce type. Les informations nominatives sont celles qui permettent l'identification directe ou indirecte des personnes physiques. Toute personne auprès de laquelle sont collectées des informations mises en oeuvre dans un système automatisé de traitement doit être préalablement informée du caractère obligatoire ou facultatif des réponses, des conséquences d'un défaut de réponse, de l'identité des destinataires de l'information, de l'existence et des modalités du droit d'accès et de rectification.

* Les dispositions du code de la propriété intellectuelle.

Toute reproduction d'un logiciel est interdite sauf autorisation préalable de son auteur (article L122.6). De même son utilisation doit être autorisée et suppose la conclusion d'un contrat de licence. Toute reproduction ou utilisation non autorisée constitue un délit de contrefaçon.

Les données telles que les textes, les images, les sons, sont également protégées par le droit d'auteur dès lors qu'elles sont originales. Leur utilisation, reproduction ou exploitation sont soumises au même régime que celui des logiciels. Certains textes ou images portent des mentions copyright qui rappellent que ceux-ci sont protégés par des droits d'auteur. Cependant à contrario l'absence de mention copyright ne signifie pas que l'utilisation des textes ou image est libre. Par ailleurs , les bases de données, entendues comme recueil d'œuvre, de données ou d'autres éléments indépendants disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou autres, bénéficient d'un statut juridique qui leur est propre (loi n°98-536 du 1° Juillet 1998). Ce dernier sanctionne notamment l'extraction de la totalité ou d'une partie substantielle du contenu d'une base de données, et sa réutilisation par mise à disposition du public sans autorisation de son producteur.

* L'obligation de discrétion professionnelle (article 26 de la loi du 13 juillet 1983 portant statut de la fonction publique) s'applique dans l'usage des outils de traitement automatisé de l'information.
Il est rappelé qu'en matière commerciale comme en matière administrative, le principe est celui de la liberté de la preuve, qui peut être rapportée par tous moyens. Un message électronique ou un enregistrement de fichier peuvent donc constituer des preuves susceptibles d'engager la responsabilité de l'administration et de l'utilisateur.

* Le secret des correspondances.

Selon le code pénal art. 226-15 « Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.

Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions »

> Un arrêt du 2 octobre 2001 de la chambre sociale de la Cour de Cassation précise « Le salarié a droit même au temps et au lieu de travail, au respect de sa vie privée ; celle-ci implique en particulier le secret de ses correspondances ; l'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié ou 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 »

* La protection de l'ordre public s'applique également à l'usage des moyens informatiques et de télécommunication.

> Selon le code pénal article 227-24 : « Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la

dignité humaine, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur. (…). »

Article 227-23 « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de trois ans d'emprisonnement et de 45000 euros d'amende. (…) »

* La protection des systèmes informatiques.

Selon le code pénal :

Art. 323-1 « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15000 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 deux ans d'emprisonnement et de 30000 euros d'amende. »

Art. 323-2 « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45000 euros d'amende »

Art. 323-3 « 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 trois ans d'emprisonnement et de 45000 euros d'amende. »

* les procédures administratives et les procédures pénales sont indépendantes

* la circulaire n° 2000-90 du 11/12/00 relative à l 'amélioration des conditions d'exercice des droits syndicaux et du dialogue social au sein des services du METL précise au chapitre I-2-c les conditions d'accès aux nouvelles technologies de l'information et de la communication par les organisations syndicales et prévoit la mise en œuvre d'une convention cosignée par l'administration et les organisations syndicales.

3) Sécurité

* Chaque agent est identifié au moment de sa connexion sur le réseau informatique par son "login". La table des login est créée par le SII. Le login de l'agent reste actif pendant la durée de présence de l'agent dans le service. Seuls les administrateurs du réseau informatique ont la possibilité de créer un tel login utilisable dans le réseau du CETE Méditerranée.

* Chaque utilisateur utilise un mot de passe associé à son login. Ce mot de passe est strictement personnel et confidentiel et ne doit en aucune raison et pour quelque motif que ce soit être divulgué à une tierce personne (que cette personne soit un collègue de travail, un supérieur hiérarchique ou un administrateur du réseau). Le mot de passe doit être composé d'un minimum de 8 caractères et doit être changé régulièrement. Il est de plus fortement recommandé de ne pas utiliser de vocable trivial ou ayant un lien avec la personnalité de l'agent, de ne pas inscrire ce mot de passe à proximité visible du poste de travail et utiliser des caractères et des chiffres.

* Les mots de passe des comptes administrateurs sont conservés par le service informatique interne sous l'autorité de l'AQSSI. Ces mots de passe sont connus exclusivement par les techniciens du Service Informatique Interne et les CLI auxquels les fonctions d'administration du réseau ont été déléguées.

* Les exigences de continuité du service doivent cependant être obtenues par des règles de partage des espaces disques sur les serveurs du réseau et les règles de transfert et de partage des droits par la messagerie. Les mots de passe applications viennent s'ajouter à ce mot de passe login pour privilégier l'accès à certaines fonctions logicielles essentiellement aux ayants droit.

Le passeport intranet s'inscrit dans cette seconde catégorie de mot de passe afin de permettre l'accès privilégier aux ressources de l'intranet en fonction du droit attribué à l'agent selon ses fonctions.

* Les mots de passe au démarrage de l'ordinateur sont prohibés sauf exception sur certains postes dont les données hébergées en local nécessite un grand niveau de sécurité. L'AQSSI est seul habilité à désigner les ordinateurs entrant dans ce champ d'exception. La liste est mise à jour régulièrement et les mots de passe sont conservés par le service informatique sous enveloppe cachetée consignée dans une armoire forte.

* Chaque utilisateur doit assurer la sauvegarde des données de son poste de travail. La sauvegarde peut être faite sur les disques partagés des serveurs de départements. Les chefs d'unités doivent s'assurer de la réalisation des sauvegardes des données nécessaires au bon fonctionnement de l'unité ; ils peuvent trouver un appui auprès des CLI pour le suivi des mesures de sauvegardes.

* Les postes de travail sont équipés d'antivirus dont la signature est mise à jour à chaque démarrage du poste de travail. Chaque utilisateur doit réinitialiser régulièrement son poste de travail afin de recharger la signature antivirus. Il est interdit de désactiver les logiciels antivirus sauf consignes particulières données pour des raisons techniques de compatibilité logicielle.

4) Confidentialité des données

* Les fichiers possédés ou créés par les utilisateurs sont réputés à usage professionnel, que ceux-ci soient accessibles ou non par d'autres agents, à l'exception de ceux qui pourraient être enregistrés dans des dossiers identifiés formellement comme personnels ou confidentiels. Le fait qu'un tiers, dans le cadre de ses attributions (administrateurs du réseau local ou correspondant local informatique) ait la possibilité de lire ou modifier un fichier ne lui en donne pas cependant le droit.

* Sur les espaces réseaux ouverts à une population cible, il est réputé acquis que chaque agent autorisé en accès d'écriture, a droit de modifier tout ou partie du fichier. Il le fait en concordance avec ses missions et dans le cadre d'un travail collaboratif avec son auteur.

* Afin d'éviter le piratage de logiciels, des règles sur les formats de fichiers peuvent être édictées quant à l'enregistrement de fichier sur les espaces disques du réseau ou des postes de travail. Le contrôle de ces espaces et des formats de fichier uniquement pourront être faits sous l'autorité de l'AQSSI. Celui-ci pourra alors demander expressément à l'agent concerné de détruire immédiatement les fichiers incriminés.

5) Messagerie

* Tout agent qui dispose d'un poste de travail dispose d'une adresse de messagerie professionnelle à son nom (en « equipement.gouv.fr »). Il peut également avoir accès à la BAL d'unité ou à une BAL fonctionnelle, selon les dispositions définies par le chef d'unité.

* La messagerie est destinée à un usage professionnel ; cependant un usage raisonnable dans le cadre des nécessités de la vie courante et familiale est toléré, à condition que l'utilisation du courrier électronique n'affecte pas le trafic normal des messages professionnels.

* Les stagiaires et vacataires ne peuvent avoir une telle boite aux lettres mais peuvent disposer d'une adresse en « i-carre.net ». Ils sont soumis aux mêmes règles d'usage que les agents du CETE.

* L'utilisation de la messagerie doit respecter les règles qui figurent dans la directive du ministère « circulaire n° 2000-14 du 18 février 2000 ». Les principaux éléments de cette circulaire qui régissent l'emploi de la messagerie sont les suivants :

Tout courrier officiel doit être transmis à partir d'une BAL d'unité.
Tout message intéressant le service et reçu dans sa BAL individuelle doit être retransmis à sa hiérarchie.
Il convient de doubler par courrier papier les messages qui engagent l'administration (toutefois une circulaire commune avec le ministère de l'Intérieur précise les modalités d'emploi de la messagerie avec les préfectures).
La gestion des BAL d'unités doit être prévue afin d'assurer la continuité du service.
L'envoi de messages à plus de 300 destinataires extérieurs est interdit.

* La sauvegarde des messages des boites aux lettres individuelles est de la responsabilité de l'agent. Celles des boites aux lettres d'unité ou fonctionnelles relèvent de la responsabilité du chef d'unité concerné.

Le partage des agendas électroniques ne s'oppose pas à l'usage du « mode privé » pour des parties de l'agenda d'un agent correspondant à sa vie privée.

6) Internet

Tous les agents ont accès aux serveurs et informations disponibles sur le Web.
*L'accès à Internet se fait par l'intermédiaire du réseau du CETE. Tout autre accès est proscrit.

* Le droit d'accès est délivré nominativement et peut être retiré. Il est interdit de donner ce droit d'accès à un tiers.

* Seuls ont vocation à être consultés les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle sous réserve que la durée de connexion n'excède pas un délai raisonnable et présente une utilité au regard des fonctions exercées. Une consultation ponctuelle et dans des limites raisonnables pour un motif personnel des sites internet dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs et ne mettant pas en cause l'intérêt et la réputation du CETE, est tolérée.

* Seules les participations aux forums et aux discussions interactives professionnelles sont autorisées : les agents y participant doivent garder à l'esprit leur obligation de réserve inhérente à leur statut de fonctionnaire. Il est rappelé en effet que l'usage des nouvelles technologies peuvent être utilisées à des fins de preuve par des tiers, aussi une grande rigueur

dans des réponses données doit être apportée car pouvant engager la responsabilité du service et par là-même de l'État.

* Tout téléchargement ou accès à un site de ce type (FTP) doit se faire dans le cadre des missions attribuées à l'agent. En cas de contrôle, ce dernier doit pouvoir justifier le recours à un tel usage. Il est rappelé qu'un téléchargement hasardeux peut gravement endommager le poste de travail voire une partie du réseau.

7) Protection des données et contrôle de l'utilisation de l'informatique

* L'autorité qualifiée de la sécurité des systèmes d'information (AQSSI) du CETE nommé par arrêté ministériel est également chargé du droit d'accès et de la protection des données personnelles sur le lieu de travail.

Il est seul habilité à :

→ autoriser en cas de nécessité absolue de service et sur demande écrite du responsable hiérarchique concerné :

- le changement de mot de passe réseau d'un agent,

L'agent en sera informé au préalable ; en cas d'impossibilité de le joindre, il en sera informé dès que possible.

→ demander des contrôles nominatifs de l'usage de l'Internet à partir des enregistrements instaurés avec un proxy et qui portent sur le compte réseau connecté, le temps passé, l'heure de connexion et les sites visités ; ces enregistrements sont conservés pendant 6 mois ; ce traitement fait l'objet d'une déclaration à la CNIL ; le SII chargé de ce traitement ne peut en communiquer les résultats par écrit qu'à l'AQSSI. ;

→ seules des statistiques sur le temps de connexion par service seront produites régulièrement et diffusées aux chefs de département ainsi qu'aux agents qui en feront la demande pour leur compte de connexion.

→ transmettre les données d'un agent à toute autorité légale qui en fait la demande écrite dans le respect des lois.

* Les CLI et le SII, sous l'autorité de leur hiérarchie, peuvent vérifier que la structuration et le contenu des postes de travail respectent les éléments du présent règlement.

Glossaire :

- AQSSI : Autorité Qualifiée de Sécurité des Systèmes d'Information.
- ASSI : Agent de sécurité des Systèmes d'Informations.
- BAL : Boite Aux Lettres électronique (Mélanie)
- CLI : Correspondant Local Informatique
- CNIL : Commission Nationale Informatique et Libertés
- CTPS : Comité Technique Paritaire Social
- FTP : File Transfert Protocol (protocole de téléchargement de fichier)