Cas 13 : Ville de V.

Nicolas
CONGIU

DOSSIER 1 : AUDIT DE L'EXISTANT **6 points**

1. Quels sont les problèmes au sein de la Mairie de V. évoqués par les personnels de la Direction Informatique ?

La Mairie de V est une collectivité territoriale située dans la commune Bretonne de V possède un système d'information et donc un réseau informatique avec intranet, des données, applicatifs, connexion Internet, messagerie, etc. Le service informatique est séparé en 5 services : la Direction Informatique qui gère l'ensemble des 4 services informatiques, les Études et Système d'Information et Gestion, les Infrastructures et systèmes, les Réseaux et sécurité et enfin, les Chargés de mission projets transversaux. D'autres directions sont présentes pour gérer la finance, les ressources humaines et la construction. La Mairie emploie environ 1 000 agents disséminés sur plusieurs sites à travers la ville.

L'objectif de la Mairie de V comme toutes les mairies est de satisfaire les besoins quotidiens de la population. Ses attributions sont multiples : état-civil, urbanisme et logement, écoles et équipements, activités culturelles, santé et aide sociale, police, etc.

Néanmoins, d'après le compte-rendu de la réunion organisée avec les personnels de la Direction Informatique, il existe des problèmes au sein de la Mairie de V.

Les agents stockent sur leur poste de nombreux documents personnels tels que des photos de vacances, vidéos, mail. Cela pose un problème de surcharge des serveurs inutiles en plus de causer des risques de pertes de données si les serveurs sont surchargés de données car ceux-ci ne peuvent plus sauvegarder en doublon les données. On rappelle que les doublons de données servent en principe à éviter des pertes de données importantes pour la Mairie.

Le problème se multiplie pour en devenir un danger pour les systèmes d'information de la Mairie de V puisque parfois les employés de la Mairie diffuse, dépose et par ce biais multiplie l'infection des postes par des fichiers contenant des virus. Cette infection oblige les techniciens à réparer les postes ce qui fait perdre du temps à la mairie sur ses missions principales citées précédemment en plus de mettre en péril les données sensibles de la Mairie.

Il est à souligner que le personnel est sensibilisé oralement de ces risques mais certains continuent à faire des actes dangereux et à infecter les postes.

2. Les agents ont-ils le droit d'utiliser à des fins personnelles les moyens informatiques mis à leur disposition dans le cadre professionnel ?

Dans le cadre professionnel, les employés de la Mairie de V disposent de moyens informatiques. Certains d'eux l'utilisent pour des activités extra-professionnelles comme le téléchargement de photos de vacances ou de vidéos. On peut définir également d'activités extra-professionnelles la consultation de site en dehors du travail comme les réseaux sociaux, les jeux etc. Cet ensemble d'activité qui semble faire perdre de la productivité à la mairie (employé peu

travailleur, ordinateurs et serveurs infectés par des documents vérolés, perte de temps à cause des services informatiques défectueux, …) peut être remis en question sur sa légalité.

L'utilisation personnelle des outils peut être exceptionnelle pour certains salariés (urgence personnelle à traiter par exemple) mais pour d'autres, elle est quotidienne. Selon une étude publiée par Olfeo en 2016, les salariés français passent 1h15 par jour, soit un mois par an, à utiliser Internet à des fins personnelles (Facebook, Youtube, Le Bon Coin, sites de voyages…) ce qui engendre une baisse de productivité de 17,6%.

D'après le Figaro, l'utilisation d'internet à usage personnel est généralement tolérée au sein de l'entreprise, par le biais d'une charte informatique, qui n'est généralement pas très précise, même si «la grande majorité des entreprises en ont rédigé une», explique Virgine Devos, avocate associée chez August & Debouzy. Pour autant, l'utilisation du web ne doit pas être exercée de manière abusive. Internet doit être utilisé de manière «raisonnable», selon la CNIL (Commission Nationale de l'Informatique et des Libertés), qui ne précise pas pour autant le délai que peut y consacrer un salarié.

«Il n'existe aucun cadre juridique spécifique à cette problématique», confirme Virgine Devos. «La question se règle au cas par cas». Pour ce faire, les juges prennent en compte plusieurs critères, à savoir la fréquence de la connexion ainsi que sa durée. Le moment choisi entre également en ligne de mire: la faute est moins importante si elle est commise au cours de la pause déjeuner. Enfin, l'impact de ces connexions sur la productivité du salarié est comptabilisé.

Pour les sanctions, «tout dépend de l'ancienneté du salarié et de la qualification de la faute», selon Virgine Devos. Première étape, l'avertissement, qui peut ensuite conduire à une mise à pied de l'employé. Ce dernier est ainsi dispensé de venir travailler. En contrepartie, les jours où il ne travaille pas sont déduits de son salaire. Plus grave, l'usage excessif d'Internet peut constituer un motif de licenciement.

Néanmoins, la loi garantit à chacun le droit au respect de sa vie privée y compris lorsque le salarié est, dans l'entreprise, sous la subordination de l'employeur (article 9 du Code civil).

Selon ce principe, l'employeur ne peut pas s'immiscer dans les affaires personnelles du salarié. Toutefois, de par son pouvoir de direction, l'employeur a le droit de contrôler et de surveiller l'activité des salariés pendant le temps de travail, mais à condition de respecter leurs droits fondamentaux et libertés individuelles (article L. 1221-1 Code du travail).

Une exemple du 13 juin 2013, dans une affaire concernant une salariée qui s'était connectée pendant les heures de travail, quasi-quotidiennement et à plusieurs reprises par jour, durant une quinzaine de jours, sur un site sur lequel elle se livrait à une activité commerciale, ainsi que sur des sites communautaires tels que "Facebook" et qui avait commis des erreurs, négligences et omissions dans l'exercice de ses fonctions, la Cour d'appel de Pau a dit que le licenciement reposait sur une cause réelle et sérieuse. Le conseil de prud'hommes avaient précédemment jugé qu'il y avait dans cette affaire absence de cause réelle et sérieuse de licenciement pour faute grave.

Des sanctions sont donc possibles, l'employeur peut prendre des mesures, dès lors qu'elles sont nécessaires et proportionnées. Il est admis par exemple que le salarié utilise son téléphone

professionnel à des fins personnelles, si cette pratique se limite à des appels de brève durée, en cas d'urgence à traiter. Dans le cas contraire, le salarié peut être sanctionné. Les sanctions peuvent s'élever d'une mise à pied jusqu'à un licenciement pour faute grave. Néanmoins, si le travail est correctement effectué et que l'utilisation à titre personnelle n'impacte pas la mairie, l'employé n'est pas sanctionnable, cela serait contre productif pour l'employeur.

sources :
https://www.ouest-france.fr/economie/emploi/droit-du-travail/peut-on-utiliser-son-ordinateur-a-des-fins-personnelles-au-travail-ouest-france-vous-repond-7001461
https://www.legisocial.fr/vie-entreprise/surveillance-des-salaries/controle-utilisation-materiel-ntic-entreprise.html
https://www.editions-tissot.fr/actualite/droit-du-travail/l-abus-dans-l-utilisation-du-materiel-informatique-a-des-fins-personnelles-justifie-un-licenciement-pour-faute-grave
https://www.lefigaro.fr/vie-bureau/2016/03/24/09008-20160324ARTFIG00157-utilisation-d-internet-a-des-fins-personnelles-au-travail-un-flou-juridique.php
https://www.village-justice.com/articles/surfer-sur-internet-pendant-vos-heures-travail-sport-dangereux,39369.html
https://licenciementpourfautegrave.fr/internet-au-travail-faute-grave/

3. Quelle solution est envisagée par Mr DMZ pour résoudre les problèmes évoqués ? Expliquer. A qui pourrait être confiée, dans l'organigramme de la ville de V., le pilotage de la mise en œuvre de cette solution ?

La solution proposée par Mr DMZ est de mettre en place une charte informatique. La charte informatique est un texte élaboré par l'organisation qui souhaite réglementer l'usage des systèmes d'information de ses salariés, agents, membres ou adhérents (entreprise, association, administration...).

Il s'agit généralement d'un document se présentant sous la forme d'un règlement intérieur imposé unilatéralement par l'organisation. Le choix dont disposent les employés, membres ou adhérents est d'accepter les conditions proposées ou d'interrompre tous liens avec l'organisation.

La mise en place d'une charte informatique dans une entreprise permet de fixer les règles d'utilisation des outils informatiques par les salariés, mais aussi de prévoir des sanctions en cas de violation de ces règles. Sa mise en œuvre est par ailleurs recommandée par la Commission Nationale de l'Informatique et des Libertés (CNIL).

Généralement intégrée au règlement intérieur de la société (ou rajoutée en annexe de ce règlement), la charte informatique peut aussi être intégrée au contrat de travail (la première solution est toutefois préférée).

Comme mentionné à l'introduction du cas et annexe 3, le responsable de la charte informatique est donc le directeur du Pôle Ressource.

sources :
https://www.cnil.fr/fr/controles-de-la-cnil-une-charte-pour-tout-comprendre
https://www.codeur.com/blog/charte-informatique-entreprise/

Cas 13 : Ville de V.

Nicolas
CONGIU

---

https://www.journaldunet.fr/management/guide-du-management/1201309-charte-informatique-rgpd-cnil/

DOSSIER 2 : PRÉALABLE À L'ÉLABORATION DE LA CHARTE INFORMATIQUE

4. Quels sont les principes fondamentaux de droit du travail que doit respecter l'élaboration d'une charte informatique ?

La CNIL peut exprimer un avis sur tout projet de charte informatique, plus particulièrement sur l'aspect « Protection des données personnelles ». Cependant, une entreprise n'a pas l'obligation de déclarer sa charte informatique à la CNIL.

Il y a toutefois des dispositions légales à respecter. Comme le stipule l'article L1121-1 du Code du travail, les restrictions des libertés individuelles imposées par la charte informatique entreprise doivent être justifiées au regard de la fonction du salarié ou de l'objectif poursuivi par l'employeur.

La charte informatique doit aussi expliquer aux salariés les moyens de surveillance informatique mis en place pour suivre leurs activités. Il peut s'agir d'un dispositif de filtrage de leur messagerie ou du contrôle des pages web qu'ils visitent.

La charte doit se conformer à la loi. L'article L1222-4 du Code du travail plus précisément. Ce dernier dispose que les informations personnelles des salariés, collectées par un dispositif, ne peuvent être récupérées qu'à condition que ce dispositif soit connu des salariés de l'entreprise.

Source:
https://www.sortlist.fr/blog/charte-informatique/
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006900785
https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072050/LEGISCTA000006189417?init=true&page=1&query=L1222-4&searchField=ALL&tab_selection=all&anchor=LEGIARTI000006900861#LEGIARTI000006900861
https://www.cnil.fr/fr/rgpd-en-pratique-proteger-les-donnees

5. Quels sont les points importants à prévoir dans une charte informatique EXEMPLES ?

Pour bien encadrer l'utilisation des nouvelles technologies de l'information et de la communication (NTIC), il est recommandé de faire figurer les informations suivantes :

-Le rappel des règles de protection des données et les sanctions en cas de non-respect.
-Le champ d'application de la charte (par exemple, les moyens d'authentification qui sont utilisés au sein de l'entreprise, les règles de sécurité auxquelles les employés doivent se conformer, etc).

-Les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition (poste de travail, équipements nomades, espaces de stockage individuel, etc).
-Les conditions d'administration du système d'information.
-Les responsabilités et les sanctions encourues en cas de non-respect de la charte.

De plus, pour certaine situation courante comme emmener son matériel personnel, il est important de fixer des règles :

L'utilisation du matériel personnel :

L'utilisation par le salarié d'outils personnels (ordinateur, téléphone, etc.) dans le cadre de son travail est un point délicat.

En effet, une telle pratique est à la fois périlleuse pour la sécurité des données de l'entreprise, mais menace aussi le respect des informations personnelles de l'employé.

S'il est préférable d'interdire tout bonnement l'utilisation de matériels personnels, une autre solution consiste à mettre en place un espace « hermétique » sur l'appareil du salarié, dans lequel seront stockées les données et les applications à usage professionnel.

Cela permet à l'entreprise d'exercer un contrôle sur les activités du travailleur sans pour autant accéder à la totalité de ses données.

Les moyens de surveillance :

La surveillance des activités des salariés par l'employeur est soumise à certaines limitations qu'il faut connaître.

D'abord, s'il est possible d'accéder les connexions, les fichiers et les mails personnels de l'employé, cela ne peut être fait qu'en sa présence.

L'utilisation d'un dispositif de contrôle des courriers électroniques ou encore des activités sur internet est permise à condition :

-D'avoir consulté les représentants du personnel ;
-D'avoir préalablement informé les salariés ;
-D'avoir fait une déclaration à la CNIL.

L'utilisation de la messagerie électronique :

L'utilisation des emails au sein de l'entreprise doit aussi être réglementée dans le cadre de la charte informatique.

Il peut notamment s'agir de mesures de confidentialité à respecter (par exemple, ne jamais mentionner certaines informations sensibles par mail).

Il peut aussi s'agir de limiter la taille des pièces jointes pouvant être reçues ou envoyées par mail.

Concernant l'utilisation de la messagerie électronique professionnelle à des fins privées, elle n'est pas interdite.

Toutefois, le salarié doit clairement identifier les mails personnels (sans quoi, ils seraient considérés comme professionnels et l'employeur aurait alors le droit de les consulter). Pour ce faire, il peut par exemple créer un répertoire dédié dans sa boîte mail.

L'accès à internet à des fins personnelles :

En principe, l'accès à internet à des fins personnelles dans le cadre professionnel est toléré dans les limites du raisonnable.

La charte informatique peut cependant prévoir une liste de sites (ou de catégories de sites) que les salariés n'ont pas le droit de visiter. Elle peut aussi interdire le téléchargement de certains fichiers.

Les sanctions possibles :

La charte informatique peut prévoir les sanctions applicables en cas de non-respect des règles énoncées. Cependant, celles-ci ne doivent pas être contraires à la loi (en particulier le Code du Travail) ni être trop excessives.

Le licenciement est une sanction envisageable, la méconnaissance et le non respect de la charte informatique pouvant constituer une faute grave.

Des règles création et de gestion des mots de passe :

Point très important ! La charte informatique doit intégrer la formation et la sensibilisation sur l'importance de choisir un mot de passe fort. Pensez à y inclure des règles pour créer et modifier les mots de passe.

Ce document doit également inclure des exigences spécifiques en matière de complexité et de longueur des mots de passe. Il doit sensibiliser les employés sur le risque d'utiliser un mot facile ou d'y inclure des informations personnelles.

L'accès à distance :

Dans un contexte de popularisation du télétravail, la charte informatique doit définir un cadre. Cela permet de minimiser les risques de piratage ou d'espionnage.

La charte informatique doit donc inclure des dispositions concernant l'envoi ou la réception d'emails et de l'utilisation des ressources intranet. L'entreprise peut exiger, de la part de l'employé en déplacement, un accès VPN, l'installation des logiciels anti-malware et l'usage des systèmes d'exploitation récents.

Par exemple, les employés ne doivent pas :

-Se livrer à des activités illégales sur leur accès à distance
-Permettre à des utilisateurs non autorisés d'utiliser leur appareil de travail
-Connecter des appareils personnels aux outils professionnels

La charte informatique doit également imposer la déconnexion lorsqu'ils laissent leur appareil seul, et l'interdiction de se connecter à d'autres réseaux lorsqu'ils sont connectés au réseau interne.

Ce document peut aussi inclure des règles de connexion au Wifi, notamment pour les collaborateurs régulièrement en déplacement. Ces derniers, amenés à se connecter à des Wifi publics, doivent être sensibilisés aux bonnes pratiques pour sécuriser leurs connexions.

Une politique de gestion de crise :

La politique de gestion de crise doit faire partie de la charte informatique. Elle décrit la réponse de l'entreprise à un incident de cybersécurité.

Elle doit détailler le rôle de chaque membre de l'équipe, les moyens et ressources à utiliser pour identifier et récupérer les données compromises. Les phases de la réponse aux incidents sont les suivantes :

-La préparation
-L'identification
-Le confinement
-L'éradication
-La récupération
-Le post-incident

L'objectif de cette politique est d'encourager la réactivité des employés en les informant sur la procédure à suivre en cas de violation de données ou d'exposition à une faille de sécurité.

La maintenance des systèmes informatiques

Comme tous les outils, les systèmes informatiques ont besoin d'une maintenance régulière. Pour réduire au minimum les interruptions et les coûts liés à la défaillance du matériel et des logiciels, il convient d'inclure, dans la charte, des calendriers et des processus de maintenance régulière.

-Quand et comment la maintenance informatique aura-t-elle lieu ?
-Comment le personnel sera-t-il informé ?
-Quels types d'interruptions de service peuvent être évités ?

Ainsi, les collaborateurs pourront anticiper ces périodes.

La signature des salariés de l'entreprise

Une charte informatique n'est complète qu'au moment où les salariés décident de la signer. Cela montre qu'ils ont pris connaissance des informations rédigées, qu'ils sont d'accord avec et qu'ils respecteront les règles. Leur vigilance est renforcée.

Cette signature donne également une valeur juridique au document. Une fois approuvées, ils n'auront d'autre choix que d'appliquer les règles édictées par la charte.

sources :
https://www.cigref.fr/archives/entreprises-et-cultures-numeriques/wp/wp-content/uploads/2015/08/Rapport-CIGREF-INESJ-2015-cellule-de-crise.pdf
https://www.codeur.com/blog/charte-informatique-entreprise/
https://www.eurecia.com/blog/charte-informatique-entreprise/
https://www.cnil.fr/fr/rgpd-en-pratique-proteger-les-donnees

6. Comment rendre la charte informatique opposable aux salariés ?

Afin de pouvoir prendre une mesure disciplinaire à l'encontre d'un salarié, l'employeur doit établir que celui-ci a commis une faute. L'article L.1331-1 du Code du travail dispose ainsi que « constitue une sanction toute mesure, autre que les observations verbales, prise par l'employeur à la suite d'un agissement du salarié considéré par l'employeur comme fautif […] ». La sanction prononcée doit être proportionnée à la faute invoquée.

Dans les entreprises de plus de vingt salariés, l'établissement d'un règlement intérieur est obligatoire (article L.1311-2 du Code du travail). Or, c'est dans ce règlement intérieur que l'employeur doit fixer « les règles générales et permanentes relatives à la discipline, notamment la nature et l'échelle des sanctions qu'il peut prendre » (article L.1312-1 3° du Code du travail).

Dans le cadre des mesures de sécurité informatique, si l'employeur entend sanctionner un salarié n'ayant pas respecté une mesure de sécurité, il lui faudra prouver que les consignes de sécurité lui ont effectivement été communiquées. La charte informatique peut alors servir d'élément de preuve.

C'est pour cette raison que la charte informatique est souvent annexée au règlement intérieur. En effet, l'opposabilité de la charte informatique aux salariés suppose qu'elle soit annexée au règlement intérieur de l'entreprise et qu'elle respecte la même procédure, notamment :

la saisine pour avis du Comité Social et économique (CSE) (article L.1321-4, alinéa 1er du Code du travail),
le dépôt au greffe du conseil de prud'hommes du ressort de l'entreprise ou de l'établissement concerné (article R.1321-2 du Code du travail),
la communication à l'inspection du travail, jointe à l'avis du CSE (article L.1321-4, alinéa 3 du Code du travail) .

Une fois le règlement intérieur dûment validé, il devra être porté à la connaissance des personnes ayant accès aux locaux par tout moyen (article R.1321-1 du Code du travail).

Cas 13 : Ville de V.

Nicolas
CONGIU

Une autre façon de faire prendre connaissance de la charte informatique est de la faire signer par l'ensemble des collaborateurs.

Sources :
https://www.agilit.law/droit-technologie-et-informations-donnees-personnelles/charte-informatique-pas-opposable-salarie-pas-connaissance/
https://www.avocats-mathias.com/droit-du-travail/charte-informatique-pourquoi
https://www.journaldunet.fr/management/guide-du-management/1441343-sanctions-en-cas-de-non-respect-de-la-charte-informatique-reglement-interieur/

DOSSIER 3 : RÔLE DES ADMINISTRATEURS RÉSEAU

7. S'agissant des moyens de contrôle, vous construirez 5 diapositives présentant :

- **Les raisons d'être des dispositifs de contrôle.**
- **Les types de dispositifs de contrôle existant au sein de la ville de V.**
- **Les règles à respecter lors de la mise en place de ces dispositifs. (liens internet)**
- **Les sanctions possibles pour la ville de V. en cas de non-respect de ces règles.**
- **Les sanctions possibles pour les agents en cas de violation de la charte.**