



Divulgence, contrôle : les collectivités et le risque Internet

Une interview réalisée par Henri Colomb

Pour Maître Féral-Schuhl, avocate spécialiste d'internet, la politique du laisser-faire pratiquée par de nombreuses entreprises privées avec leur salariés est difficilement concevable pour les administrations, car elle les expose à de nombreux risques juridiques.

Qu'est ce que l'irruption d'internet change, ou risque de changer, au plan juridique pour les collectivités locales ?

L'internet est un moyen privilégié d'échanges entre les agents et les administrés. Cette dématérialisation des échanges soulève les questions usuelles : la preuve, la responsabilité du contenu, l'intégrité, l'authentification...

L'[ordonnance de 2005 relative aux échanges électroniques](#) entre les usagers et les autorités administratives ainsi qu'entre les autorités administratives, est venue fixer le cadre juridique des conditions dans lesquelles les administrations, dont les collectivités locales, doivent ainsi échanger avec les administrés. Conformément à cette ordonnance, deux textes ont été publiés, détaillant les obligations des personnes publiques : le RGI, [référentiel général d'interopérabilité](#) et le RGS, [référentiel général de sécurité](#).

Existe-t-il en matière d'utilisation d'internet des obligations particulières pour les personnels d'administrations ou de collectivités ?

Ces personnels ont une activité particulière pouvant justifier un encadrement strict de l'utilisation d'internet et de l'outil informatique. La plupart des entreprises adoptent la politique du « laisser-faire », la connexion aux réseaux sociaux ou à des sites de ventes en ligne pouvant être effectuée via la connexion professionnelle. Une telle politique est difficilement concevable dans l'administration où est traditionnellement exercée une plus grande surveillance sur l'utilisation de l'outil informatique par les agents.

En revanche les moyens mis à la disposition des responsables informatiques sont identiques : une « charte informatique », appelée aussi « charte éthique », ou « charte internet », qui n'est pas obligatoire mais vivement recommandée, pourra énoncer le principe de l'interdiction, et organiser les conditions dans lesquelles un contrôle des agents sera susceptible d'être exercé.

La dernière jurisprudence dans ce domaine concerne une société privée, mais la solution peut être transposée à l'Administration : la chambre sociale de la Cour de cassation vient de valider un licenciement intervenu suite à la découverte d'images pornographiques sur l'ordinateur d'un salarié, alors même que la charte interdisait un tel comportement. La charte l'ayant précisé, ce comportement était donc incontestablement fautif et susceptible d'entraîner une sanction pouvant aller jusqu'au licenciement.

Quels sont, selon vous, les "points à risque" sur lesquels les collectivités doivent être le plus vigilantes ?

Ils sont nombreux mais j'en identifie deux sur lesquels les collectivités doivent être particulièrement vigilantes :

- d'abord la **divulgarion d'information** : les collectivités ne sont pas à l'abri de la diffusion involontaire ou volontaire d'informations qui peuvent revêtir un caractère stratégique ou confidentiel. Les fonctionnaires sont soumis à un devoir de réserve et de discrétion, qui leur interdit de diffuser ce genre de contenus. L'usage d'internet accroît incontestablement le risque et Wikileaks en est une parfaite illustration, puisque le site aurait été alimenté par des informations en provenance de l'administration américaine.
- ensuite le **défaut de contrôle des contenus** : les agents devront faire attention aux contenus téléchargés ou diffusés par l'intermédiaire d'internet. En matière de droit d'auteur, ils doivent veiller à ne pas mettre en ligne des photographies ou des contenus sur lesquels ils n'auraient pas d'autorisation des ayants droits. En matière pénale, ils ne doivent pas télécharger, conserver ou publier des contenus illicites.

Une collectivité peut-elle juridiquement défendre sa "e-réputation" ?

La « e-reputation » est un sujet en vogue. Cette notion concerne à la fois la communication qu'une administration réalise pour son compte sur la toile (présentation de son rôle et de ses missions par exemple sur son site internet), mais également les propos ou contenus qui la concernent, et sur lesquels son pouvoir de contrôle est beaucoup plus restreint.

Les moteurs de recherches gardent en mémoire ces contenus souvent sans limite de durée, ce qui fait qu'une critique peut ressurgir des années après avoir été publiée. Défendre sa e-réputation est donc désormais de plus en plus difficile, d'autant qu'assurer une veille permanente sur internet est quasiment impossible.

Toutefois, une collectivité, comme toute personne morale, conserve les moyens de droit classiques pour faire retirer un contenu injurieux ou diffamant. Et elle peut, conformément à la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004, solliciter, par notification aux hébergeurs, le retrait de ces contenus.

A-t-elle un droit de regard sur les messages échangés par ses agents ?

En tant qu'employeur, une collectivité pourra avoir un contrôle sur l'outil informatique qu'elle met à disposition de ses agents. C'est ce qu'on appelle la cybersurveillance. L'employeur doit néanmoins respecter deux règles : la transparence et la proportionnalité. Cela signifie qu'il doit informer les agents et les représentants du personnel du dispositif mis en œuvre, et respecter la proportionnalité, c'est-à-dire être en mesure de démontrer que le dispositif est proportionné à la finalité du contrôle.

En revanche, le respect de la vie privée des salariés fait que, si le caractère personnel d'un message reçu dans la messagerie professionnelle d'un agent est spécifié, la collectivité, sauf circonstances particulières, ne pourra le lire ou se prévaloir directement de ce courriel qu'en prenant certaines précautions. Par exemple, être préalablement autorisé par un juge et n'ouvrir cet e-mail personnel qu'en présence de l'agent concerné.

Une collectivité peut-elle sanctionner ses agents, voire les licencier, pour leur expression sur le web ?

Les agents jouissent, comme les salariés, de la liberté d'expression. Néanmoins, cette liberté d'expression ne doit pas dépasser le devoir de réserve des agents territoriaux. Et ce devoir de réserve va plus loin que le simple devoir de loyauté et de discrétion des salariés du privé. Ainsi, un agent ne peut faire de sa fonction l'instrument d'une propagande.

Le cas récent du site Wikileaks 13 en est une illustration : un agent a été suspendu de ses fonctions par le Conseil général des Bouches-du-Rhône pour avoir créé un site visant à dénoncer notamment des actes de corruption ou d'abus de pouvoir des pouvoirs publics locaux. Sa hiérarchie a en effet jugé que les critiques formulées allaient au-delà de la liberté d'expression.

Il existe effectivement pour tout agent de la fonction publique une obligation de réserve, consacrée par la jurisprudence du Conseil d'État, qui interdit au fonctionnaire de faire de sa fonction l'instrument d'une propagande quelconque.

Les agents des collectivités peuvent-ils s'exprimer en toute liberté sur les réseaux sociaux ?

Les réseaux sociaux sont d'abord et avant tout un outil de communication. Il convient de toujours conserver à l'esprit que publier un contenu n'est pas un acte anodin. Par ailleurs, internet n'est pas un espace sans règle ou non régi par le droit. En tout état de cause les propos injurieux ou diffamants sont sanctionnables.

La vigilance doit de manière générale porter à la fois sur les contenus diffusés, mais également sur les destinataires des contenus, c'est-à-dire les paramétrages adoptés par celui qui publie. Ainsi, en octobre 2008, le conseil de prud'hommes de Boulogne a jugé justifié le licenciement de salariés pour des propos injurieux postés sur Facebook avec une autorisation d'accès aux « amis des amis ».

Selon le paramètre du compte, le réseau social relève de la sphère privée ou publique. Toutefois, un groupe restreint ne garantit pas la confidentialité : chacun des amis peut partager avec les autres personnes du réseau. On ne leur interdit pas de réutiliser l'information.

Le meilleur conseil pouvant être donné aux agents est assurément celui de rester vigilants et modérés dans leur propos.

Mini CV

Christiane Féral-Schuhl est avocate au barreau de Paris et spécialisée dans le domaine des TIC au sein du cabinet Féral-Schuhl / Sainte-Marie. Elle est notamment l'auteure aux éditions Dalloz du volumineux ouvrage « Cyberdroit, le droit à l'épreuve d'internet », dont la 6ème édition 2011-2012 vient d'être publiée (Cyberdroit 2011-2012, Praxis Dalloz, 1124 pages, 58 euros) . Elle anime aussi le site d'actualité juridique cyberdroit.fr