

**Vers un droit à la déconnexion au travail ?**

Le 15 septembre dernier, Bruno Mettling, DGA d'Orange, a remis à la ministre du Travail un rapport relatif aux effets du numérique sur les outils, l'environnement et l'organisation du travail. L'une des préconisations du rapport est de réfléchir à un droit à la déconnexion des salariés, face au phénomène du « blurring » qui consiste à rester connecté et disponible chez soi, après le travail, et à répondre aux e-mails en pleine nuit par exemple.

**Rejet par la CNIL du recours de Google**

Suite à la consécration par la Cour de Justice de l'Union Européenne d'un droit au déréférencement permettant aux internautes de demander aux moteurs de recherche le retrait de résultats inappropriés, la CNIL a mis en demeure publiquement Google, en juin dernier, d'appliquer cette décision sur toutes les versions de son moteur de recherche, européennes ou non. La CNIL vient de rejeter le recours gracieux de Google, qui devra dès lors se conformer à ces demandes.

**Publication du projet de loi sur le numérique**

Le projet de loi sur la « République numérique » a été publié samedi 26 septembre par Axelle Lemaire, secrétaire d'État chargée du numérique. Le texte prévoit notamment l'ouverture et la gratuité de l'accès aux données des administrations publiques, la consécration du principe de « neutralité du net », ainsi qu'un renforcement du « droit à l'oubli » pour les mineurs. Les internautes ont la possibilité de proposer des modifications du texte jusqu'au 17 octobre.

# Usage d'Internet en entreprise : sécurité, organisation et filtrage

**LES FAITS**

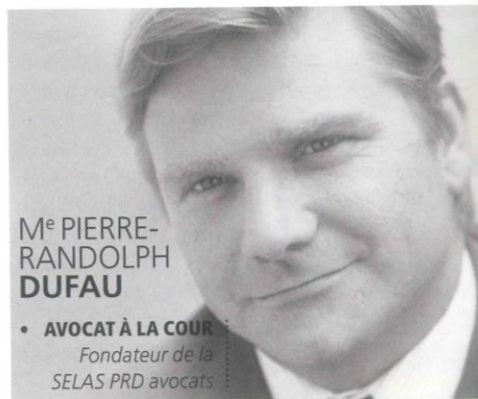
*Networking, hubworking, web 2.0, BYOD, Web TV d'entreprise, télétravail, sous-traitance ou recours à des free-lances, tour d'horizon des enjeux de l'usage d'Internet et des pratiques à imposer.*

**LES RISQUES ENCOURUS PAR L'ENTREPRISE**

L'utilisation d'Internet au bureau fait peser sur l'entreprise un certain nombre de risques, sur le plan légal comme technique. Au niveau juridique, il convient de rappeler que, selon l'article 1384 al. 5 du Code civil, l'employeur est responsable des dommages causés par ses salariés. L'entreprise peut également voir sa responsabilité engagée sur le plan pénal, notamment en cas d'accès à des sites comportant des contenus illicites (téléchargement illégal, etc.). Diverses obligations de « déconnexion » face au phénomène du « blurring » apparaissent aussi, par exemple dans les entreprises relevant de la convention collective dite « Syntec ». Sur le plan technique, l'usage d'Internet par les salariés ou tiers autorisés peut également aggraver la vulnérabilité de l'entreprise face à des logiciels malveillants ou des hackers cherchant à s'introduire sur le réseau pour piller ou détruire d'éventuelles données confidentielles. Les entreprises doivent donc désormais prévoir des outils de filtrage afin d'organiser et de sécuriser l'utilisation du réseau.

**CADRE JURIDIQUE ET BONNES PRATIQUES DU FILTRAGE**

La mise en œuvre de moyens de sécurisation et de filtrage peut constituer dans certains cas une obligation légale. L'article 336-3 du Code de la propriété intellectuelle impose par exemple au titulaire d'un accès Internet de protéger son réseau contre le piratage d'œuvres protégées par le droit d'auteur, à moins de commettre une négligence caractérisée pouvant être sanctionnée par une amende contraventionnelle de 5<sup>e</sup> classe d'un montant de 7 500 euros pour les personnes morales. Dans ces conditions, la CNIL reconnaît aux employeurs la possibilité de limiter l'utilisation d'Internet en entreprise.



M<sup>e</sup> PIERRE-RANDOLPH DUFU

• **AVOCAT À LA COUR**  
Fondateur de la SELAS PRD avocats

Sur le plan pratique, il convient dès lors de rattacher une charte informatique au règlement intérieur, laquelle peut interdire l'accès à certaines catégories de sites, aménager des durées raisonnables ou des horaires de consultation des réseaux sociaux ou organiser l'utilisation de matériels informatiques personnels avec le développement du BYOD. Outre la désignation d'un administrateur réseau, une solution technique de filtrage doit également être mise en place afin d'authentifier les utilisateurs, gérer l'accès aux contenus des sites et messageries instantanées via des listes noires ou des mots-clés, et proposer une analyse de l'activité ciblée. La CNIL a rappelé que les salariés doivent être informés des dispositifs et modalités de contrôle mis en place, et si des sanctions disciplinaires peuvent en découler. De surcroît, en application de l'article L2323-32 du Code du travail, il convient de consulter et d'informer le comité d'entreprise de la mise en œuvre de tels dispositifs. Enfin, si la solution de filtrage permet de relever les connexions de chaque salarié, le traitement de données doit faire l'objet d'une déclaration normale auprès de la CNIL. ∞

**CE QU'IL FAUT RETENIR**

**Il relève de la responsabilité du DSI de mettre en place une charte informatique doublée de systèmes de filtrage spécifiques et appropriés aux évolutions techniques. Il convient de prévoir un dispositif opposable non seulement aux salariés, aux tiers habilités à travailler dans l'entreprise, ainsi qu'aux cocontractants.**