Parc d'Activités Schweitzer
26 rue du Bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEIL

FILTRAGE WEB

OBJET DE LA FICHE

Ce document a pour but de vous informer sur vos droits et obligations envers vos collaborateurs, relatif à la mise à disposition de l'accès Internet de votre société

PREVENTION

Lorsque vous mettez à disposition de vos collaborateurs un accès Internet via le réseau de votre entreprise, le dirigeant est responsable des agissements des utilisateurs. Au même titre qu'un fournisseur d'accès Internet.

Par conséquent vous devez, en cas d'utilisation illicite de votre Internet fournir aux autorités les logins permettant d'identifier l'utilisateur concerné.

Exemples d'utilisation illicite d'internet :

- Visite de sites classés « Terrorisme »
- Téléchargement illicite de logiciels, films, musqies etc…
- Consultation et/ou téléchargement de contenus à caractère pédophile …

LEGISLATION

〉 CE QUE DIT LA LOI HADOPI SUR LE FILTRAGE INTERNET EN ENTREPRISE

La loi dite Hadopi (Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet) protège les droits des auteurs et des ayants droit en sanctionnant la pratique du téléchargement illégal sur Internet. Autorité administrative indépendante, Hadopi est chargée de faire respecter la loi via la Commission de Protection des Droits (CPD).

Publiées en juin et octobre 2009, ces lois reposent sur un système de riposte graduée pouvant conduire à la suspension de la connexion Internet s'il est constaté le téléchargement de contenus en violation des dispositions du Code de la propriété intellectuelle (CPI).

En application de l'article L.336-3 du CPI (modifié par la loi Hadopi 2), **le chef d'entreprise a :** *« l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par le droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits ».*

L'enjeu majeur pour une entreprise concerne l'aspect juridique. La loi française est très précise en matière d'obligation et les jurisprudences récentes montrent que les conséquences peuvent être désastreuses en matière de productivité et d'image publique des entreprises et des établissements scolaires.

〉 QUI EST RESPONSABLE DANS LE CAS D'UNE UTILISATION ABUSIVE D'INTERNET ?

En entreprise, les salariés ont un droit d'utilisation d'Internet à des fins personnelles pour un **usage dit « raisonnable »**. Cette sphère d'intimité sur le lieu de travail ne peut être remise en cause. Ce droit doit être reconnu dans la charte informatique de l'entreprise, car dans le cas contraire cela entrainerait sa nullité aux yeux de la loi.

L'entreprise (et par extension, son représentant) est responsable civilement et / ou pénalement de la façon dont son système d'information est utilisé en interne, quels que soient les utilisateurs. Il est donc indispensable de mettre en place des outils de filtrage Internet permettant d'assurer la bonne utilisation de son système d'information.

LES ASPECTS JURIDIQUES LIÉS AU FILTRAGE INTERNET

〉 OBLIGATION DE MOYENS

L'entreprise doit mettre en œuvre les moyens nécessaires pour interdire l'accès à des sites illégaux, notamment en ce qui concerne les téléchargements de fichiers ou logiciels piratés.

Il s'agit de protéger le réseau par exemple contre la consultation de sites racistes, négationnistes, l'achat de produits dont la vente est interdite sur Internet (certains médicaments, alcool, tabac).

〉 OBLIGATION DE SECURISATION DE SON RESEAU CONTRE LE PIRATAGE

L'entreprise doit mettre en œuvre les moyens nécessaires pour interdire l'accès à des sites illégaux via une solution de filtrage de contenus Web notamment.

Il s'agit de protéger le réseau par exemple contre la consultation de sites racistes, négationnistes, l'achat de produits dont la vente est interdite sur Internet (certains médicaments, alcool, tabac).

〉 OBLIGATION DE CONSERVATION DES LOGS

Lors de la mise en place d'une solution de filtrage Internet, l'entreprise doit s'engager à conserver les données de connexion (LOG) pendant 1 an.

〉 OBLIGATION DE MISE EN PLACE D'UNE CHARTE INFORMATIQUE

La mise en place d'une solution de filtrage Web avec identification des utilisateurs doit s'accompagner de la mise en place d'une charte informatique qui doit être portée à la connaissance des salariés et du comité d'entreprise.

〉 OBLIGATION DE DECLARATION A LA CNIL

Lorsque la solution de filtrage Internet mise en place collecte des informations nominatives, il est nécessaire de faire une déclaration à la CNIL. En revanche, cette déclaration n'est pas obligatoire si le filtre Internet ne permet pas un contrôle individualisé des salariés. Pour en savoir plus, consultez la fiche pratique de la CNIL sur le contrôle de l'utilisation d'Internet et de la messagerie.

L'employeur est un «fournisseur d'accès»

En effet, l'employeur donne l'accès aux réseaux numériques à ses employés. De ce fait, l'article 9 de la Loi pour la Confiance dans l'Economie Numérique (Lcen) du 21 Juin 2014 dispose que «toute personne assurant une activité de transmission de contenus sur un réseau ou de fourniture de l'accès à un réseau» bénéficie d'une responsabilité atténuée dans la Loi. Or, il est d'interprétation unanime, que cette activité de «fourniture d'accès» n'est aucunement réservée dans la Loi aux opérateurs de communications électroniques (ex opérateurs de télécoms) ou à ceux qui techniquement fournissent l'accès. Cette définition dans la Lcen s'applique, comme pour les hébergeurs, à tous ceux qui sont dans la fonction de fournir un accès aux réseaux. Tel est le cas de l'employeur pour ses employés.

Or, ce statut de fournisseur d'accès bénéficie d'un régime de responsabilité atténuée qui a une contrepartie, celle de conserver les «données de nature à permettre l'identification de quiconque a contribué à la création de contenu» (article 6 Lcen). Pour mémoire, le défaut de conservation est puni d'un emprisonnement d'un an et de la peine maximale de 75 000 euros d'amende. La durée de conservation des données a, quant à elle, été fixée à une année à compter de leur enregistrement.

Ainsi donc, en dehors de toute cybersurveillance au sens où nous l'avons entendu ci-avant, l'employeur serait donc astreint à conserver les données de trafic pendant un an à compter de leur enregistrement. L'objectif avoué du législateur est de permettre à la justice de requérir dans le cadre de sa traque aux délits civils et / ou pénaux, une identification. C'est ce que rappelle une décision abondamment commentée : «il y a lieu de constater que le législateur français, ainsi que la législation européenne le lui permettait, a souhaité trouver un équilibre en conférant à l'opérateur [cette affaire mettait au prise un opérateur] une responsabilité atténuée en contrepartie de sa collaboration pour la conservation de données qu'il est dans l'obligation de produire sur injonction d'une autorité judiciaire quelle qu'elle soit, civile ou pénale.»

〉 CE QUE DIT LA LOI SUR LA RESPONSABILITE CIVILE DES ENTREPRISES

Art 1383 Code Civil
" Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence "

Art 1384 du Code Civil " On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre […]

PROTEGER L'ENTREPRISE DE L'USAGE D'INTERNET FAIT PAR LES COLLABORATEURS

Avec le Web 2.0, les possibilités d'attaque et de piratage du réseau informatique sont de plus en plus nombreuses et les salariés connectés à Internet depuis le réseau de l'entreprise pour effectuer des paiements en ligne, consulter des sites potentiellement à risques, télécharger des fichiers ou toute autre action, mettent en danger la sécurité de leur entreprise.

Les conséquences de ces intrusions peuvent être catastrophiques pour une entreprise : blocage des ordinateurs, ralentissement du réseau, fuites d'informations confidentielles, récupération des contacts du carnet d'adresses, propagation de spams, phishing, etc.

62% des entreprises françaises victimes d'au moins un incident de sécurité en 2012 - étude menée par PwC

Selon l'étude "Global State of Information Security Survey 2014" de PwC, les cyberattaques sont le type d'attaque les plus redoutées par les dirigeants. 2013 a ainsi vu s'accroître le nombre d'incidents dans ce domaine. 27% des dirigeants interrogés en France affirment avoir connu plus de 10 incidents de sécurité en 2012, contre 21% en 2011.

Avec l'émergence de nouvelles technologies, les menaces liées à la sécurité de l'information ne cessent de croître. Pour se protéger des menaces et sécuriser leurs données, les entreprises installent des solutions antimalwares au niveau des postes de travail des salariés.

Pour une protection optimum, l'entreprise doit tout d'abord mettre en place **des outils de filtrage d'URL pour bloquer l'accès à certains sites**, certaines catégories de sites aux contenus potentiellement dangereux. Enfin cela doit s'accompagner d'un filtrage de flux qui permet de détecter les menaces, malwares au niveau de la navigation sur Internet (consultation de sites, téléchargement de fichiers).

LUTTER CONTRE LA SATURATION DE LA BANDE PASSANTE AVEC UN FILTRE INTERNET

On assiste depuis le développement d'Internet et des vidéos à une forte croissance du besoin en bande passante par utilisateur. Les nouvelles pratiques professionnelles comme le Cloud Computing participent également à cette évolution.

Des ressources importantes sont nécessaires pour la mise en cache des vidéos en ligne, ce sont les consommateurs de ce type de contenus qui sont à l'origine de la plus grande partie du trafic. Ce trafic vidéo compte pour plus du tiers pour les réseaux fixes et environ 40 % pour les réseaux mobiles, selon le rapport publié en 2012 par le ministère de l'Economie et des Finances sur Les besoins en bande passante et leur évolution.

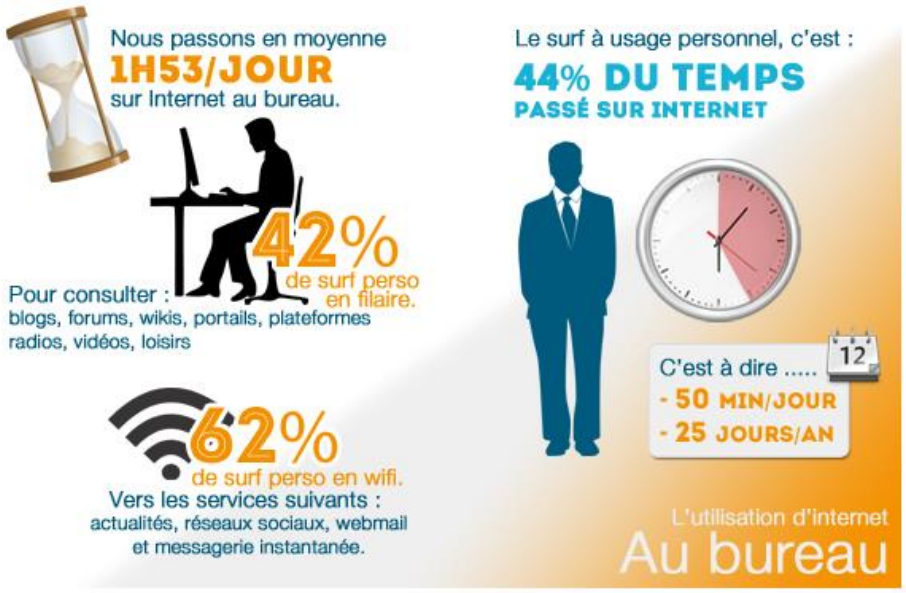
LE FILTRAGE INTERNET ET L'IMPACT SUR LA PRODUCTIVITE

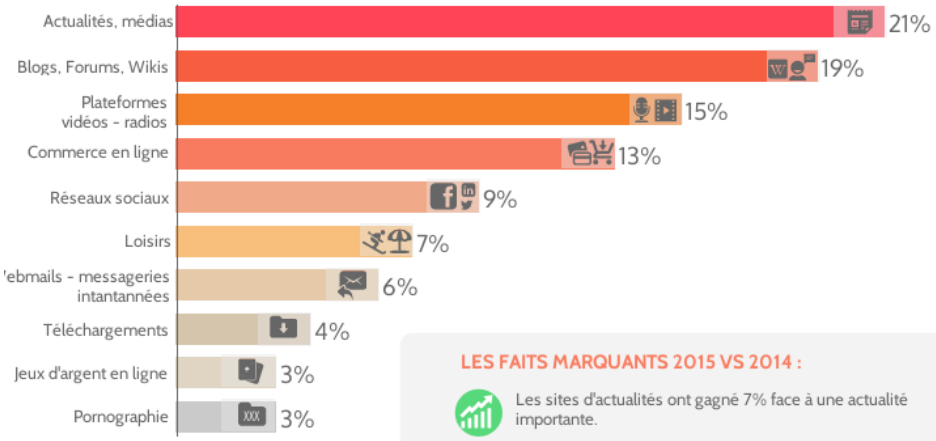
L'impact de l'utilisation d'Internet à titre personnel en entreprise constitue un réel coût en matière de productivité, de performance et de sécurité des réseaux.

L'utilisation d'Internet en entreprise est devenue incontournable pour obtenir des données de marché, se tenir au courant des actualités industrielles ou financières, mettre en place des actions commerciales en ligne, faire une recherche sur les concurrents, chercher un fournisseur etc. Mais Internet représente également un moyen de distraction pour les salariés et par extension, un risque réel de baisse de leur productivité.

E-mails personnels, ventes en ligne, réseaux sociaux comme Facebook ou Twitter, plateformes de vidéos en ligne… les salariés passent de plus en plus de temps personnel sur Internet au bureau. Selon nos estimations, les salariés passent en moyenne 1 heure par jour sur Internet à des fins personnelles.

La consultation de sites extra-professionnels est facilement indexable à une utilisation plus importante de la bande passante, mais aussi au grand nombre d'heures de travail perdues chaque année, ce qui représente une baisse de productivité et donc une perte pour l'entreprise.





LES FAITS MARQUANTS 2015 VS 2014 :

Les sites d'actualités ont gagné 7% face à une actualité importante.

+ 3% pour les blogs, forums et wikis

Le commerce en ligne reste stable mais important.

- 3% pour les réseaux sociaux avec des internautes qui se connectent directement via les applications sur smartphone tout comme les webmails ou encore les sites de jeux d'argent en ligne.