L'édito du TiPi :

Le juriste et le technicien ou le délicat mariage de la carpe et du lapin

Souvent, l'édito du TiPi est l'occasion pour un membre du Cabinet de s'attarder sur un point de droit particulier intervenu dans les mois précédents. Ainsi, je pourrais vous parler des débats parlementaires concernant le projet de Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure ou encore de l'excellente initiative du Secrétariat d'Etat à l'Economie Numérique sur le label IdéNum ou l'identité numérique multi-services. Mais le Cabinet en reparlera prochainement.

Je voudrais simplement raconter une anecdote intervenue lors d'une Conférence le 2 juillet dernier, « *L'IPRA (Intellectual Property Rights Analysis) pour renforcer la confiance dans les logiciels issus de la recherche* ». A l'issue de la séance de questions réponses, face à un parterre de techniciens et d'ingénieurs, l'un d'entre eux a indiqué ne pas comprendre l'importance apportée par les juristes concernant la gestion des éléments de preuve. Pour ce dernier, la preuve informatique (binaire) était suffisante, absolue et il ne comprenait pas l'acharnement qu'ont tous les juristes à se préconstituer des preuves (relatives car humaines). Il a fallu patiemment disséquer le raisonnement juridique afin de lui faire comprendre qu'aussi irréfutable soit-elle, une preuve informatique doit permettre de convaincre un juge qui, souvent, n'est pas féru d'informatique ou un expert nommé par le juge à qui il convient de faciliter la tâche en prévoyant des documents techniques explicatifs du processus. Inversement, le juriste doit exposer au technicien les règles de droit applicables afin d'en tirer les conséquences utiles (et techniques) pour le projet.

Cette anecdote est venue renforcer le sentiment que chacun des membres du Cabinet partage. Techniciens et juristes utilisent des termes identiques (preuve, signature, copie, …) mais sans qu'ils recouvrent le même contenu.

C'est ce qui explique que le Cabinet mette un point d'honneur à mettre en place une pierre de rosette commune avec ses clients afin de faciliter le dialogue et la compréhension mutuelle.

La différence enrichit dès le moment où on sait qu'elle existe.

Pascal AGOSTI
Avocat associé
Docteur en droit

Aujourd'hui dans le TiPi :

Edito

Actualités :

- **Du côté de la signature électronique**
- **La nouvelle directive relative à la facture électronique**
- **Quoi de neuf concernant les données à caractère personnel ?**

Focus :

L'usage des réseaux sociaux dans l'entreprise et le Droit

Jurisprudences :

- **Obligation de résultat et contrat informatique**
- **Google Adwords : Google irresponsable ?**
- **Vraisemblance de la copie informatique**

Une réponse… à une question :

Que faire des BAL électroniques des anciens salariés ?

Actualités :

Du côté :

… de la signature électronique

Deux applications ont fait jour concernant le recours à la signature électronique dans l'administration. Ainsi, le décret du 18 juin 2010 applicable aux magistrats, avocats et autres professionnels concourant à la procédure pénale vient insérer le recours à la signature électronique sécurisée ou à la signature numérique, entendue comme « *signature manuscrite conservée sous forme numérique après avoir été apposée sur un écran tactile, au moyen d'un appareil sécurisé garantissant l'intégrité de l'acte dès que la signature a été enregistrée* » (art. R. 249-11 du Code de procédure pénale) pour les *actes en rapport avec la procédure pénale.*

Les modalités d'applications des deux articles R. 249-10 et R.249-11 du Code de procédure pénale seront précisées par arrêté du Garde des sceaux, notamment concernant les caractéristiques de l'appareil sécurisé.

De même, la signature électronique sécurisée sera utilisée par les agents assermentés et agréés de l'HADOPI pour leurs procès verbaux, conformément à l'article R. 331-36 du CPI introduit par le décret n°2010-872 du 26 juillet 2010.

Cette diffusion de la signature électronique dans chaque pan de l'organisation administration permettra de sensibiliser notamment les magistrats, en cas de litige portant sur ce sujet.

Décret n°2010-671 du 18 juin 2010 relatif à la signature électronique et numérique en matière pénale et modifiant certaines dispositions de droit pénal et de procédure pénale ; J.O. du 20 juin 2010, p. 1183.

Décret n°2010-872 du 26 juillet 2010 relatif à la procédure devant la commission de protection des droits de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet, J.O. du 27 juillet 2010 p. 13874.

… de la facturation électronique

La Commission européenne a présenté un rapport mettant en évidence certaines difficultés relatives à la facturation électronique en raison de l'évolution technologique. En effet, la facturation électronique se développe maintenant rapidement, notamment en raison de la croissance du commerce électronique. Or, la diversité des règles en vigueur au sein des Etats membres de l'Union européenne relative à la facturation électronique est considérée comme un frein à l'expansion de ce type de facturation. De plus, les exigences posées par la Directive 2006/112/CE entravent l'adoption de la facturation électronique, ce qui empêche les entreprises de réaliser des économies potentiellement importantes en matière de bureaucratie dans les entreprises.

Cette Directive a pour but d'accroître l'utilisation de la facturation électronique, de réduire les charges pour les entreprises, de soutenir les petites et moyennes entreprises (PME) et d'aider les États membres à lutter contre la fraude. Pour atteindre ces objectifs, la Directive a notamment pour objectif de veiller à ce que les autorités fiscales acceptent les factures électroniques dans les mêmes conditions que les factures sur support papier en vertu de l'application du principe de non discrimination de l'écrit électronique. Elle vise également à supprimer de la Directive 2006/112/CE les obstacles entravant le recours à la facturation électronique. En effet, il est nécessaire d'accroître le recours à la facturation électronique, en cessant de faire des signatures électroniques avancées ou de l'échange des données informatisées des conditions indispensables à l'envoi de factures électroniques.

Directive 2010/45/UE du Conseil du 13 juillet 2010 modifiant la directive 2006/112/CE relative au système commun de taxe sur la valeur ajoutée en ce qui concerne les règles de facturation, J.O.U.E L. 189 du 22 juillet 2010, p. 1 et s.

… et des données à caractère personnel

Circulez : il y a tout à voir

La CNIL a mis en ligne sur son site un nouveau document sur le **transfert de données à caractère personnel vers des pays tiers à l'Union européenne** qui remplace (et annule) le Guide sur le transfert de données de juin 2008. Très clair et riche d'enseignements sur les questions que se posent les exportateurs de données, en attendant la révision de la Directive 95/46/CE, mais on a le temps ...

Tout savoir sur les transferts internationaux de données, 23 septembre 2010, www.cnil.fr

Etes-vous au courant ? Identification indirecte et Electricité

En juillet 2009, dans le cadre de l'adoption de règles communes pour le marché intérieur de l'électricité (directive 2009/72/CE du 13 juillet 2009) et pour le marché intérieur du gaz (directive 2009/73/CE du 13 juillet 2009), il a été prévu que les Etats membres de l'UE modernisent leurs réseaux de distibution, en les invitant notamment à **mettre en place des systèmes de mesure ou réseaux intelligents**. Les directives ont fixé l'échéance pour l'évaluation des coûts de cette mise en place au 3 septembre 2012. En ce qui concerne l'électricité, si l'évaluation s'avère favorable, 80% des clients devront être équipés de compteurs électriques intelligents (ou « smart grid ») avant fin 2020. Il doit être ici souligné qu'en France, l'**article 8 de la loi n°2009-967 du 3 août 2009 « Grenelle 1 »** préconise, dans un même souci d'économie d'énergie, la **généralisation des compteurs électriques intelligents.**
Ces compteurs permettront de mesurer très précisément la consommation électrique d'un foyer, de la relever pratiquement en temps réel et de la transmettre au distributeur du réseau d'énergie (ERDF pour l'électricité en France). Une meilleure élaboration de la facturation, l'adaptation de la production d'énergie à la consommation effective des utilisateurs, la réduction de la pollution ainsi que la réalisation d'économies sont autant d'arguments qui militent en faveur de ces dispositifs. Toutefois, la CNIL (brève du 5 août 2010) et la CRE - Commission de Régulation de l'Energie - ont soulevé les risques de traçage des usagers dans la mesure où les informations sur la consommation d'énergie peuvent être révélatrices de leur vie privée (horaires de réveil et de coucher, sensibilité à la chaleur ou au froid liée aux périodes de chauffauge ou d'usage de la climatisation, consommation d'équipements électriques, …). La CRE a sollicité la CNIL pour participer au groupe de travail sur les compteurs intelligents afin d'apporter des recommandations sur la protection des données à caractère personnel ainsi indirectement collectées… *A suivre* …

Directive 2009/72/CE du Parle

abrogeant la directive 2003/54/CE, J.O.U.E L. 211 du 14 août 2009, p. 55 et s.

Directive 2009/73/CE du Parlement européen et du

abrogeant la directive 2003/55/CE, J.O.U.E L. 211 du 14 août 2009, p. 94 et s.

Je consomme donc je suis … protégé

Le Conseil National de la Consommation (CNC) a rendu public courant septembre un ***Avis accompagné d'un Rapport sur la protection des données personnelles des consommateurs***, problématique dont il avait été saisi fin 2008 par M. Chatel alors secrétaire d'Etat en charge de la consommation. D'un point de vue formel, l'Avis est un recueil de 27 propositions recensant les points d'accord entre professionnels et associations de consommateurs et le Rapport vient préciser certains de ces points. En substance, les propositions regroupées sous trois axes, ont trait à la nécessité de :

- sensibiliser les consommateurs sur la protection de leurs données ;
- développer la culture « protection des données » au sein des entreprises, notamment avec une meilleure connaissance du cadre légal ;
- renforcer le rôle des acteurs de la protection, en l'occurrence la CNIL et le CIL.

Même si la CNIL a d'ores et déjà souligné le bien fondé de l'ensemble de ces propositions, force est de constater qu'elles sont très générales voire superflues. En tout état de cause, leur effectivité devra être appréciée sur l'année à venir, le CNC s'étant engagé à dresser un bilan pour le premier semestre 2012.

Avis du Conseil National de la Consommation sur la protection des données personnelles des consommateurs, 18 mai 2010, disponible à l'adresse :

http://www.finances.gouv.fr/conseilnationalconsommation/avis/2010/180510protection_donnees_perso.pdf

Focus :

L'usage des réseaux sociaux dans l'entreprise et le Droit

Phénomène inconnu il y a encore moins de cinq ans, l'usage des réseaux sociaux en ligne a crû depuis de façon exponentielle. Ainsi, le dirigeant de Facebook, le plus célèbre d'entre eux, a annoncé en juillet 2010 qu'il avait plus de 500 millions de comptes actifs… et envisageait de fêter le chiffre du milliard dès courant 2011 alors qu'il n'est ouvert à tous les internautes de plus de 13 ans que depuis septembre 2006.

Appartenant à la catégorie plus large des média sociaux (dont les jeux Massivement Multijoueurs en Ligne, les univers virtuels, le micro-blogging, les partages de photo ou de vidéo, etc.), les services de réseaux sociaux en ligne permettent à l'internaute de construire, de représenter ou d'étendre ses relations sociales, qui partent d'un point commun (éducation, activité professionnelle, nationalité, etc.) et se nourrissent de créations et de partages de contenus ou d'activités.
Au plan juridique, la définition du réseau social est venue du Groupe dit « de l'article 29 », rassemblant les régulateurs européens en matière de protection des données à caractère personnelle, Groupe qui utilise[1] le terme de « *services de réseautage social* » (SRS) entendus comme : « *des plates-formes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs* ».
Le G29 mentionne également que ces SRS « *partagent certaines caractéristiques :*

- *les utilisateurs sont invités à fournir des données à caractère personnel permettant de donner une description ou un « profil ».*
- *les SRS mettent également à disposition des outils permettant aux utilisateurs de mettre leur propre contenu en ligne (contenu généré par l'utilisateur tel que des photos, des chroniques ou des commentaires, de la musique, des vidéos ou des liens vers d'autres sites) ;*
- *les «réseaux sociaux» fonctionnent grâce à l'utilisation d'outils mettant à disposition une liste de contacts pour chaque utilisateur avec une possibilité d'interaction.* »

En pratique, on distingue classiquement 4 grands types de réseaux :

- les réseaux d'anciens (le défunt Sixdegrees.com[2], Copains d'avant, etc.) ;
- la recherche de l'âme sœur (Meetic, Match.com) ;
- le développement du réseau professionnel (Linked In, Viadeo, Plaxo, Xing') ;
- et les services dédiés aux échanges et à la socialisation entre personnes aux affinités communes (Skyrock, Facebook, Myspace, Fourquare).

Autant d'activités donnant lieu à des consultations fréquentes par les salariés, y compris sur leurs lieux de travail, comme le montrent fréquemment les listes des sites les plus couramment consultés au sein des entreprises.
Or, se connecter sur Facebook ne permet plus seulement de mettre son profil à jour ou de regarder et commenter celui des autres. Grâce aux partenariats et à Facebook Connect, on peut utiliser des systèmes de messageries électroniques, s'interfacer avec des outils de partage d'informations ou de contenus, voire… jouer (poker, jeux de rôle en ligne, mondes virtuels tels que Farmville, etc.).

Face à ces nouveaux usages, l'entreprise est souvent partagée à l'heure actuelle concernant l'attitude qu'elle doit avoir vis-à-vis de la consultation des SRS par ses salariés. La problématique de la productivité joue un rôle important mais la mise en cause éventuelle de la responsabilité juridique de l'entreprise est un élément qu'il ne faut pas négliger. Face à ses usages internes, le paradoxe pour l'entreprise quant à son attitude peut être d'autant plus grand qu'elle use elle-même en général très largement de toutes les potentialités que les SRS lui offrent dans le cadre de ses activités (publicité, communication avec les clients, gestion de l'image, etc.) et dont les problématiques juridiques feront certainement l'objet d'un prochain article, tout comme l'étude des problématiques juridiques que soulève la création d'un SRS interne à une entreprise.

Formations - Conférences :

Formation FNTC Dématérialisation, P. Agosti, 23 septembre 2010, Paris.

Assises de la sécurité, Table ronde, Utilisation des équipements informatiques personnels dans l'entreprise, E. A. Caprioli, 6 octobre 2010
Procès Rezosocio, E. A. Caprioli, 8 octobre 2010, Palais des congrès, Monaco

ARAB ICT legal and legislation FORUM, E. A. Caprioli, **Ecrit et preuve électronique dans une perspective internationale**, 3 Novembre 2010, Beyrouth.

LEXPosia 2010 : La fraude sur l'Internet, E.A. Caprioli, F. Coupez, 19 novembre 2010, Paris, Palias Brogniard.

Comundi : Cybersurveillance des salariés, F. Coupez, 24 et 25 novembre 2010, Paris.

(1) Avis 5/2009 sur les réseaux sociaux en ligne adopté le 12 juin 2009, disponible sur http://ec.europa.eu/justice/policies/privacy/index_en.htm

(2) Premier site de réseau social en ayant toutes les caractéristiques, il tenait son nom de la théorie « *It's a Small world* » du Docteur Stanley Milgram établissant en 1967 que chaque individu n'est au maximum qu'à 6 degrés de relations d'un autre être humain pris au hasard.

Juridiquement et de façon synthétique, l'usage des réseaux sociaux dans l'entreprise révèle essentiellement des problématiques de droit du travail et de droit de la sécurité des systèmes d'information.

I. Les services de réseaux sociaux en ligne et droit du travail

A. Pendant la phase de recrutement

La tentation est grande, non seulement pour la DRH, mais surtout pour toutes les personnes ayant à intervenir à un moment ou à un autre dans un processus de recrutement (managers directs, managers en ligne hiérarchique plus haute, éventuellement collègues, etc.), d'aller consulter la mine d'informations que les SRS peuvent contenir sur un candidat au recrutement (que ces informations soient d'ailleurs mises en ligne de son fait ou postées par d'autres). D'autant que certains moteurs de recherche se sont spécialisés dans la recherche dite « multiprofils » et permettent d'amalgamer les résultats des différents SRS pour donner une image considérée comme encore plus fidèle, plus complète de la personne. Comme l'indique Alex Türck, président de la CNIL, « *Les recruteurs ou même les policiers utilisent beaucoup ce genre de réseaux. La police y trouve d'ailleurs beaucoup plus d'informations que sur les fichiers des Renseignements Généraux.* »

Certes, la jurisprudence a eu l'occasion de rappeler qu'il appartenait à l'employeur « *de s'informer préalablement à la conclusion du contrat des réelles capacités professionnelles du candidat* » (CA Nancy 27 mars 2002) ou encore « *de vérifier la véracité des mentions figurant sur le CV* » (CA Montpellier 5 février 2002).

Pourtant, malgré la forte tentation qu'il peut éprouver, l'employeur ne peut utiliser de manière indifférenciée les informations mises en ligne par le candidat. Il est tenu au respect de l'art. L. 1132-1 du Code du travail[3]. Compte tenu de la nature des informations publiées sur nombre de SRS, la consultation des pages du candidat sur les Facebook et consorts, ou sur les moteurs de recherche spécialisés, apparaît être une tentation qu'il convient de refréner pour des raisons juridiques. En effet, si l'employeur tombe sur des informations qui lui donnent une bien trop mauvaise image du candidat, il aura des difficultés à ne pas en tenir compte dans le cadre du processus de recrutement, ce que l'art. L. 1132-1 l'oblige pourtant à faire.
Ainsi, une étude réalisée par le site CareerBuilder en Allemagne en 2009 a montré que 45% des employeurs recherchent le profil Facebook de leurs futurs collaborateurs pour tenter d'y déceler toute anomalie.

(3) « *aucune personne ne peut être écartée d'une procédure de recrutement […] en raison de son origine, de son sexe, de ses mœurs, de son orientation sexuelle, de son âge, de sa situation de famille ou de sa grossesse, de ses caractéristiques génétiques, de son appartenance ou de sa non-appartenance, vraie ou supposée, à une ethnie, une nation ou une race, de ses opinions politiques, de ses activités syndicales ou mutualistes, de ses convictions religieuses, de son apparence physique, de son nom de famille ou en raison de son état de santé ou de son handicap* ».

Afin de tracer des limites relativement claires sur le sujet et de répondre à ces problématiques en respectant les exigences légales, les 40 cabinets de recrutement de l'association « à compétence égale » ont signé le 12 novembre 2009 la Charte d'autorégulation « Réseaux sociaux, Internet, Vie privée et Recrutement ».
Cette charte prévoit ainsi de :
- de limiter les réseaux sociaux à la seule diffusion d'offres et avec le consentement de l'utilisateur ;
- de ne pas utiliser les réseaux sociaux comme outils d'enquête et ne pas collecter des informations d'ordre personnel, voire intime, même si elles sont rendues accessibles par les utilisateurs eux-mêmes ;
- de sensibiliser et former les recruteurs sur la nécessité de ne pas collecter ni de ne tenir compte de telles informations ;
- d'alerter les internautes sur la nécessité de veiller à la nature des informations qu'ils diffusent et au choix des personnes à qui ils souhaitent y donner accès ;
- d'interpeller les gestionnaires des sites Internet hébergeant des réseaux sociaux, des blogs, des moteurs de recherches sur l'importance d'informer très clairement leurs utilisateurs.

Le gouvernement allemand a, quant à lui, préféré une autre voie en présentant le 25 août 2010 un projet de loi sur la protection des données à caractère personnel des salariés qui vise, notamment, à interdire aux employeurs de consulter le profil Facebook et les messages.

publiés par les candidats à l'embauche (exception faite des SRS à vocation professionnelle).

Le respect de ces principes, qu'ils soient issus de professionnels du recrutement en France (autorégulation) ou du gouvernement en Allemagne, apparaît d'autant plus important qu'avec l'explosion du nombre d'abonnés à des SRS et leurs caractères internationaux, les cas d'homonymies se multiplient également… et avec les erreurs qu'ils peuvent entrainer, préjudiciables aux candidats injustement écartés, par exemple en raison d'un intérêt affiché publiquement pour les « drogues dures » ou encore « l'alcool » (alors qu'en réalité, la page est celle d'un autre).

En pratique, les contenus mis en ligne sur les SRS peuvent également attirer l'attention de l'employeur après le recrutement, alors que le salarié travaille dans l'entreprise et que, pour une raison ou une autre, les contenus mis en ligne (par lui ou par d'autres), révèlent des informations qui appellent, selon l'employeur, à une sanction (licenciement, etc.).

B. Pour fonder une sanction

Ce type de cas se multiplie à l'heure actuelle et les contentieux commencent à trouver le chemin des tribunaux. On y retrouve, par exemple, le licenciement de salariés critiquant leurs supérieurs hiérarchiques sur Facebook (un de leurs « amis » Facebook ayant relayé l'information à l'employeur). Cet exemple se rapproche d'une part des plaintes liées à la création de contenus ou de groupes diffamant ou insultant des tiers (et donc non spécifiques au monde du travail) et, d'autre part, aux contentieux où le salarié avait posté sur son blog le récit de son quotidien professionnel au grand dam de son employeur[4].
Il est difficile de tirer des enseignements de contentieux encore naissants dans ces domaines, d'autant plus que chaque cas concrets est différent du point de vue des faits, mais les principes dégagés de façon plus générale par la jurisprudence en droit du travail doivent continuer à s'appliquer :

- un salarié ne peut être sanctionné par l'employeur en raison de faits tirés de sa vie personnelle (C. cass. Soc., 14 mai 1997) ;
- ce principe ne trouve pas à s'appliquer si ces faits ont été causés par l'utilisation de l'ordinateur professionnel pendant le temps de travail (Cass. Soc., 12 mai 2010) ;
- les faits doivent être imputés au salarié de manière fiable (comment l'employeur s'est-il aperçu des contenus publiés sur Facebook ? Comment peut-il prouver qu'ils proviennent du salarié ?). Il convient en particulier de prendre en compte les hypothèses de malveillance de tiers… ou d'homonymes (cf. supra) ;
- des procédés de preuve licite de ces faits doivent avoir été mis en œuvre. Le moyen de preuve illicite n'est en effet pas accepté par les juridictions civiles et peut engager la responsabilité civile voire pénale de l'employeur (atteinte à la vie privée, le cas échéant interception de correspondance privée, etc) ;
- dans le cas de propos décrivant la vie professionnelle, ils ne peuvent être reprochés au salarié que si l'employeur est identifiable et que les propos (diffamatoires, etc.) provoquent un « *trouble objectif caractérisé au sein de l'entreprise* » (Cass. Soc., 30 juin 1992).

(4) Conseil des Prud'hommes du 29 mars 2007, affaire F 06/08171 dite « du blog de PetiteAnglaise ».

Reste la solution de la restriction des usages des SRS dans le cadre professionnel, pour éviter les hypothèses de mise en ligne de contenus qui ne nuisent pas directement à l'entreprise ou ne sont pas illicites en soit, mais altèrent l'image de l'entreprise vis-à-vis de ses clients. Celle-ci peut se fonder sur le respect du règlement intérieur de l'entreprise et plus précisément des documents tels que les chartes régissant l'utilisation des moyens électroniques de l'entreprise. Ainsi, l'utilisation de logiciels particuliers ou la connexion à des sites interdits peut être proportionnée.
A ce titre, le dernier exemple en date d'une grande entreprise restreignant l'usage des SRS est celui de la société Singapore Airlines, dont un porte-parole a indiqué début septembre 2010 : « *Our staff may of course have a blog or Facebook and Twitter account like any other member of the public (…) But our policy is clear that they must not comment on work matters about business or customers, so as to protect proprietary information as well as the privacy of other staff and our customers.* »[5]

(5) « *Notre personnel peut bien sûr avoir un blog ou un des comptes Facebook et Twitter, comme tout autre membre du public (…) Mais notre politique est claire : ils ne doivent pas commenter des questions de travail concernant les affaires ou les clients, de manière à protéger les informations appartenant à des tiers ainsi que la vie privée des autres membres du personnel et de nos clients.* ».

II. Les services de réseaux sociaux en ligne et le droit de la sécurité des systèmes d'information

A. Usage abusif et responsabilité de l'employeur

De plus, si l'employeur en vient à édicter des règles concernant les restrictions d'utilisation des moyens informatiques qu'il met à disposition à titre professionnel, c'est souvent en raison de la mise en cause de sa responsabilité juridique qu'un usage abusif par un salarié peut entrainer. Celle-ci peut être directe, par le biais de la responsabilité du préposé du fait des agissements de ses commettants (art. 1384 al. 5 du Code civil avec une large palette d'application, v. notamment Cour d'appel d'Aix-en-Provence, 13 mars 2006, SA Lucent Technologies c/ SA Escota, SA Lycos France, Nicolas B.).
Or, les SRS, en raison des contenus mis en ligne, sont les grands pourvoyeurs des faits de diffamation, incitation à la haine raciale, insultes et autres délits de presse qui, quand ils sont le fait du salarié, peuvent également entrainer la responsabilité de l'employeur. D'autant que, pour l'instant du moins, la jurisprudence considère que Facebook serait un hébergeur et à ce titre profite du régime de responsabilité atténué issu de la transposition de la directive commerce électronique du 8 juin 2000 [6].

Mais la mise en cause de la responsabilité juridique de l'employeur peut également être plus indirecte et le conduire par exemple à ne pas pouvoir résilier un contrat de protection (anti-virus en l'occurrence) si, le résiliant pour défaut de protection, on s'aperçoit que la société « *en laissant son personnel se connecter à de tels sites, a rendu, par sa faute, inefficace la protection que XXX s'était engagée à lui fournir de sorte qu'elle ne pouvait invoquer la défaillance de la protection anti-virus comme un juste motif de la résiliation des contrats* » (CA Paris, 25e ch., sect. B, 4 mai 2007, Normaction c/ KBC Lease France, DMS : JurisData n° 2007-334142 ; Comm. com. électr. 2008, comm. 30).
Sur un plan plus technique, il se trouve en effet que les SRS sont également une mine d'or pour les malware selon le « *Security Threat Report 2010* » de la société Sophos.

B. Sécurité et confidentialité : le risque venu du SRS

Concernant la sécurité, les SRS comme Facebook et autres médias sociaux comme Twitter sont ainsi considérés comme des sources de risques préoccupants[7] s'ils ne sont pas encadrés. Ainsi, pour Sophos ou encore le Cert-IST, les réseaux sociaux sont considérés comme un gros risque pour les entreprises qui les autorisent sans limite[8], en raison des risques très importants de fuite d'informations confidentielles ou encore de facilitation des attaques par ingénierie sociale.

Ces attaques sont permises non seulement en raison des défauts de sécurité de nombre de SRS, mais aussi et surtout, en raison de la richesse des informations que mettent en ligne les salariés concernant leur travail ou leur employeur. Sont particulièrement concernés ici les utilisateurs des réseaux sociaux en ligne professionnels type Linked In ou Viadeo, qui, poussés par le SRS et afin de valoriser leur profil, mettent en ligne le plus d'informations possibles les concernant. Il n'est ainsi pas rare que des organigrammes de société, des lancements de produits secrets, des rachats confidentiels ou encore des informations liées au fonctionnement intrinsèque de certains services de l'entreprise se retrouvent sur les pages des SRS professionnels, accessibles aux autres utilisateurs… qui se trouvent souvent être ses principaux concurrents !
Face à ces dangers, les entreprises intègrent des dispositions particulières dans leurs chartes règlementant l'usage des outils informatiques, voire s'ils ne peuvent l'empêcher, encadrent très finement leur utilisation dans des **« chartes d'utilisation des médias sociaux » ad hoc**. Celles-ci rappellent d'ailleurs en pratique aux salariés leur obligation de loyauté inhérente au contrat de travail (qui doit être respectée sous peine de sanction, comme doivent l'être les clauses de confidentialité signées par des prestataires externes), et viennent souvent en parallèle d'actions de formation à ces nouveaux usages (que l'employeur gagne souvent à prévoir). Les outils et procédures existent donc pour permettre la meilleure sécurité juridique possible de l'entreprise, charge à elle de se doter d'une approche claire et cohérente en matière de SRS.

(6) Voir à ce titre l'ordonnance de référé du TGI de Paris du 13 avril 2010 dans l'affaire Hervé G. / Facebook France, disponible sur http://legalis.net/spip.php?page=breves-article&id_article=2899.

(7) Dans ce domaine, Twitter a fait l'objet d'une enquête par la Federal Trade Commission (FTC), qui a abouti à un accord-sanction sur le long terme. Ce dernier a interdit à la société Twitter Inc proposant le service éponyme de « *tromper les consommateurs à propos de la protection mise en œuvre sur la sécurité, la vie privée et la confidentialité de leurs données* » et ce, pendant une durée de 20 ans. Elle l'a également contrainte à mettre en place de véritables mesures de sécurité qui garantissent l'intégrité des données de ses utilisateurs, au même titre que l'obligation de sécurité des données à caractère personnel pesant sur le responsable de traitement en France (article 34 de la loi du 6 janvier 1978 dite loi Informatique, Fichiers et Libertés). Un auditeur indépendant analysera tous les ans, pendant 10 ans, la pertinence et l'efficacité des mesures prises.
Concernant Facebook, un informaticien américain a récupéré le 27 juillet dernier, grâce à une petite application qu'il a créée, 170 millions de données à caractère personnel émanant de Facebook et correspondant à 100 millions de profils (1/5ème des membres au plan mondial). Il a ensuite publié ces données sur des sites de partages de fichiers. La seule réponse de Facebook a été de considérer qu'il n'y avait rien de grave car « *les informations que les gens ont accepté de rendre publiques existent déjà sur Google, Bing, et sur les autres moteurs de recherche, en plus de Facebook. Aucune donnée privée n'est accessible ni n'a été compromise.* ».

(8) Voir en ce sens http://www.sophos.fr/pressoffice/news/articles/2009/12/facebook.html

Jurisprudence :

Google Adwords : le critère jurisprudentiel du rôle actif de Google en question

Le système Adwords, proposé par la société Google, est un service de référencement payant qui permet à tout opérateur économique, moyennant la sélection d'un ou de plusieurs mots-clés, de faire apparaître, en cas de concordance entre ce (ou ces) mot(s) et ceux ou celui contenus dans la requête adressée par un internaute au moteur de recherche, un lien promotionnel vers son site. Durant plusieurs années, ce programme publicitaire a fait l'objet de véritables débats jurisprudentiels soulevant de nombreuses interrogations, à savoir les conséquences en cas de mot-clé préalablement déposé comme marque par un concurrent, ou encore l'identité du responsable de l'acte de contrefaçon (l'entreprise proposant ce service ou la société choisissant le mot-clé ?).

La CJUE, dans le cadre d'un arrêt en date du 23 mars 2010, a formellement exonéré la société Google de toute responsabilité quant à la mise en place de ce service. Elle a considéré que cette dernière, faute de faire usage de la marque dans la vie des affaires, ne peut voir sa responsabilité engagée pour contrefaçon de marque du fait de son service Adwords, dans la mesure où Google n'utilise pas le signe pour sa propre communication (C. Caron, *« FAQ » autour de l'arrêt Google sur les liens commerciaux*, Comm. Com. électr. n° 7, Juillet 2010, comm. 70). Ainsi, qu'il s'agisse d'une marque notoire ou non, et que le prestataire propose d'utiliser des signes qui vont présenter des produits contrefaisants ou non, Google ne peut être poursuivie sur le fondement de la contrefaçon et sa responsabilité ne peut être engagée que dans l'hypothèse où elle a joué **un rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées.** A contrario, l'annonceur, quant à lui, encourt un risque considérable. En effet, ce dernier peut être condamné pour contrefaçon (voire même pour concurrence déloyale lorsque le procédé permet à l'annonceur de détourner la clientèle de son concurrent), dans la mesure où il fait un usage du signe d'autrui dans la vie des affaires et que, dès lors que cet usage est fait par l'annonceur pour des produits ou services concurrents, il porte atteinte à la fonction d'indication d'origine de la marque utilisée à titre de mot-clé (E. Dreyer, *Un an de droit de la publicité*, Comm. Com. électr. n° 7, Juillet 2010, chron. 7).

Au niveau national, les suites de cette décision ont été visibles au travers de quatre arrêts rendus le 13 juillet dernier par la Cour de cassation. Alors que trois de ces décisions concernaient les questions préjudicielles déjà soulevées et qu'une autre opposait plusieurs entreprises d'électroménager à Google, il a été confirmé que les propriétaires de marque ne pouvaient plus faire grand chose face à Google et qu'il n'y avait plus que les annonceurs vers qui se tourner, solution qui a été enrichie par le dernier arrêt de la CJUE du 8 juillet dernier (C. Caron, *« FAQ » n° 2 autour des liens commerciaux…,* Comm. Com. électr., Octobre 2010). Désormais, les contours des droits et obligations des annonceurs sont nettement définis. Ainsi, il est impératif que ces derniers respectent l'identification d'origine des produits afin d'éviter toute interdiction de faire de la publicité pour des produits et services identiques à ceux pour lesquels la marque est enregistrée et, par ailleurs, d'être considérés comme contrefacteurs (en raison du risque de confusion). Notons que, dans la mesure où les mots-clés sont considérés comme des signes reproduits recélant des différences si insignifiantes qu'elles peuvent passer inaperçues aux yeux d'un consommateur moyen, l'annonceur risque une condamnation pour contrefaçon à l'identique (et non pas pour imitation). La nécessité de caractériser un risque de confusion n'a donc plus lieu d'être, ce risque étant admis automatiquement. Le risque pèse également sur l'annonceur, en plus de se voir condamner pour reproduction de la marque à l'identique désignant des produits identiques ou similaires à ceux désignés lors du dépôt de la marque, d'être condamné même si son annonce ne mentionne pas expressément des produits identiques à ceux qui ont été désignés par le titulaire de la marque. Il est par ailleurs possible pour l'annonceur de bénéficier de […]

Signaux de fumée (en direct du web…)

Cour de cassation, chambre sociale, 13 juillet 2010 : une société de sécurité avait été engagée pour garder les locaux de la société Thalès. Or, un des vigiles a utilisé à des fins personnelles le matériel informatique de Thalès et a provoqué une panne. **Il n'y a eu en l'occurrence qu'une seule utilisation (prouvée), mais la Cour a considéré qu'une telle utilisation, par ce salarié de la société prestataire, pendant le temps de travail et à des fins personnelles du matériel informatique de l'établissement où il était en mission, était constitutive d'une faute grave.**

http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000022491465&fastReqId=1327025340&fastPos=1

Eric Walter, **le secrétaire général de l'Hadopi**, a participé le 27 août à un tchat organisé par La Tribune **où il a spécifiquement confirmé, si le doute était encore permis, que la « réponse graduée » mise en place par la loi « vise tout type d'abonnement » et s'applique donc aux entreprises.** Il a également conseillé aux chefs d'entreprise d'adopter une charte informatique interne.

http://www.latribune.fr/technos-medias/internet/20100820trib000541008/exclusif-piratage-sur-internet-les-reponses-du-patron-d-hadopi.html

l'exemption de référence nécessaire, mais ce, seulement s'il utilise honnêtement la marque d'autrui pour vendre ses propres produits, forcément complémentaires de ceux du propriétaire de la marque reproduite. Enfin, il est possible pour l'annonceur de se prévaloir de l'épuisement des droits pour utiliser la marque d'autrui comme mot-clé. En effet, le titulaire d'une marque ne peut pas interdire à un annonceur de faire de la publicité pour la revente de produits fabriqués par ce titulaire et commercialisés dans l'Union Européenne par lui ou avec son consentement, sauf motifs légitimes (impression de l'existence d'un lien économique entre l'annonceur et le titulaire de la marque, atteinte à la renommée de la marque, atteinte à l'image, dissimulation de la marque).

La renaissance des clauses de responsabilité et l'arrêt Faurecia

Dans les négociations de contrats avec les prestataires informatiques, il est nécessaire d'accorder une attention particulière aux clauses de responsabilité, qui sont destinées à préciser les conditions dans lesquelles le prestataire informatique se voit tenu de réparer les préjudices subis par son client du fait de la mauvaise exécution ou de l'inexécution des prestations objet du contrat. Récemment, les clauses de limitation de responsabilité ont fait couler beaucoup d'encre. En effet, en matière de contentieux relatifs à des contrats informatiques, il est possible d'évoquer la célèbre affaire opposant la société Faurecia à la société Oracle.

En l'espèce, un contrat de licence a été conclu entre, d'une part, une société d'équipements automobiles (Faurecia), qui souhaitait se munir d'un logiciel de production et de gestion commerciale et, d'autre part, une société de service informatique (Oracle). Dans la mesure où le logiciel définitif n'était pas encore au point, une solution temporaire a été développée, solution qui entraîna cependant de nombreux désagréments alors même que le logiciel définitif ne fut jamais livré. Par conséquent, l'équipementier automobile Faurecia, reprochant à la société Oracle de ne pas avoir honoré le contrat, mit un terme au paiement de ses redevances. La société Oracle, quant à elle, lui opposa une clause limitative de responsabilité qui plafonnait l'indemnisation. La Cour d'appel de Paris avait, en 2008, jugé que ladite clause était valide, estimant également que la société Faurecia ne démontrait pas l'existence d'une faute lourde imputable à la société Oracle, et qui puisse tenir en échec la clause limitative de réparation.

La Cour de cassation a, le 29 juin dernier, rejeté le pourvoi formé par la société Faurecia qui avait tenté de faire casser le jugement de la Cour d'appel. La Cour de cassation affirma, dans un premier temps, que « *seule est réputée non écrite la clause limitative de réparation qui contredit la portée de l'obligation essentielle souscrite par le débiteur* », retenant ainsi la validité de la clause de l'espèce. En effet, dans la mesure où le montant de l'indemnisation prévu dans ladite clause tenait compte de la répartition du risque et que, dès lors, la limitation de responsabilité qui en résultait n'était pas dérisoire, le contenu de la clause n'était donc pas contraire à l'objet même du contrat. Dans un second temps, en déclarant que « *la faute lourde ne peut résulter du seul manquement à une obligation contractuelle, fût-elle essentielle* », la Cour de cassation rappelle que la faute lourde devant se déduire de la gravité du comportement du débiteur (*Conditions de validité d'une clause limitative de responsabilité*, JCP éd. E & A n° 27, 8 juillet 2010, act. 383, Som.), un manquement à une obligation essentielle n'est pas en principe une faute lourde et, de ce fait, un tel manquement n'exclut pas de façon automatique la clause limitative de responsabilité (B. Lamon, *Manquement à une obligation essentielle et clause limitative de responsabilité*, Expertises, Août/Septembre 2010).

Ainsi, l'enseignement majeur de cet arrêt est que le manquement à l'obligation essentielle ne suffit pas à écarter la clause limitative de responsabilité. Il est nécessaire que le juge constate par ailleurs que la clause limitative de réparation vide de sa substance l'obligation essentielle du débiteur (D. Houtcieff, *L'essentiel est dans la contradiction*, JCP éd. G, n° 28-29, 12 juillet 2010) !

Signaux de fumée (en direct du web…)

Depuis quelques années, les tribunaux ont eu l'occasion de rappeler les modalités techniques essentielles, selon eux, pour juger de la fiabilité d'un constat sur internet. **Afin de guider les huissiers dans leurs constats et d'éviter les tentatives de remise en cause systématique de ceux-ci, la norme AFNOR NF Z 67-147** *« Mode opératoire de procès-verbal de constat sur internet effectué par Huissier de justic »* a vu le jour **en septembre 2010 (le cabinet Caprioli était membre du comité de normalisation).**

http://www.boutique.afnor.org/NEL5DetailNormeEnLigne.aspx?CLE_ART=FA167706&nivCtx=NELZNELZ1A10A101A107&ts=8171319

Cette décision s'apparente à une sorte de renaissance des clauses limitatives de responsabilité. En effet, désormais, tout client mécontent souhaitant contourner les clauses limitant la responsabilité de son fournisseur se verra opposer cette décision rendue par la Cour de cassation.

Vraisemblance de la copie informatique

Mme X salariée de la société Carrefour a déclaré, le 8 septembre 2003, être atteinte d'une tendinite de l'épaule. Par décision du 1er mars 2004, la Caisse primaire d'assurance maladie des Vosges a pris en charge cette maladie considérée comme professionnelle. La société a contesté l'opposabilité de la décision de prise en charge.

La 2ème chambre civile de la Cour de cassation a rejeté le pourvoi de la société, en rappelant le pouvoir souverain d'appréciation des juges du fond concernant la valeur et la portée des éléments de preuve produits devant elle et en précisant que « [la copie de la lettre recommandée du 17 février 2004 ainsi que l'accusé de réception] *constitue*[nt] *un commencement de preuve émanant de la personne à laquelle elle est opposée et rend vraisemblable le fait allégué, même si l'entête et le pied figurant sur la lettre ne sont pas ceux qu'utilisait la caisse à l'époque, et résulte de la réédition de la lettre conservée en informatique* […] ».

On pourrait penser que cette décision est en contradiction avec celle rendue par cette même chambre le 4 décembre 2008 (CCE, Février 2009, n°19, p. 44 et s) qui avait rejeté une copie de courrier avec les mêmes problèmes d'entête et de pied de page différents. Ce n'est pas le cas car la copie du courrier était revêtue d'une signature et un accusé de réception était fourni par la CPAM. On peut, en revanche, conclure que dans cette matière comme dans d'autres, le Juge dispose d'un large pouvoir d'appréciation qui lui permet d'accepter ou de refuser tel ou tel élément de preuve et que c'est **la vraisemblance de celle-ci qui sera retenue par lui** (D. Ammar, *Preuve et vraisemblance, contribution à l'étude de la preuve technologique*, RTD. Civ. 1993, p. 499 et s.). En l'occurrence, c'est ici l'accusé de réception qui, considéré comme un commencement de preuve par la Cour d'appel, rend vraisemblable selon elle la copie du courrier.

Vie du cabinet :

Le Cabinet recherche des stagiaires pour l'entité niçoise à compter du mois de septembre pour des périodes allant de 2 mois à 6 mois :

- en cours de diplôme d'un troisième cycle de haut niveau en droit des nouvelles technologies ou d'un DJCE ;

- maîtrisant l'anglais.

Contactez le Cabinet à l'adresse suivante : contact@caprioli-avocats.com

Une réponse… à une question :

Le cabinet a sélectionné une question concernant les boîtes aux lettres d'anciens salariés

Que faire des boîtes aux lettres (BAL) électroniques des anciens salariés ?

Face à cette question complexe – et qui n'en est pas moins fréquente –, la réponse dépend en partie de l'organisation interne propre à l'entreprise concernée, ainsi et surtout que des règles qu'elle a mises en place dans sa charte informatique ou son règlement intérieur concernant l'utilisation des moyens de communications électroniques par ses salariés. Cette question doit d'ailleurs souvent être envisagée en amont, lors de la rédaction de telles chartes, afin que la réponse puisse être mise en musique facilement par l'entreprise.

Différentes régles peuvent à ce titre être prévues :

- la labellisation des messages privés ;
- la conservation d'une copie des messages emportés par le salarié pendant une durée prévue dans la charte ;
- les modalités de prise de connaissance des messages en question et le recours éventuel à un huissier de justice selon certaines conditions ;
- l'effacement par le salarié des messages privés de sa BAL avant son départ ;
- ou encore les modalités de transmission des courriers électroniques en cas de décès du salarié.

Il apparaît donc que, dans tous les cas, ces problématiques doivent être anticipées dans les chartes d'utilisation et autres Politique de Gestion des Courriers Electroniques (pour les grandes entreprises surtout) déterminant les conditions du traitement des Courriers électroniques de chaque salarié, que ce dernier fasse encore partie des effectifs de l'entreprise ou pas.

Cette rubrique est votre rubrique. Vous pourrez poser votre question à l'adresse contact@caprioli-avocats.com.

TiPi dans le détail :

La Newsletter du Cabinet Caprioli & Associés est une publication du Cabinet Caprioli & Associés.

La Newsletter est un instrument d'information et son contenu ne saurait en aucune façon être interprété comme un avis ou un conseil juridique.

Néanmoins, pour de plus amples détails sur un des thèmes abordés, n'hésitez pas à nous contacter à l'adresse suivante : contact@caprioli-avocats.com.

Toute demande de désinscription à la présente Newsletter peut être effectuée à l'adresse suivante : contact@caprioli-avocats.com.