LEXING ALAIN BENSOUSSAN
Juristendances Informatique et Télécoms
n° 136 – juin 2013

LE DEFAUT DE CURIOSITE DU CLIENT ET LA MAUVAISE FOI DU PRESTATAIRE

La réticence dolosive rend toujours excusable l'erreur provoquée

- Ce principe énoncé pour la première fois en 2001 (1) a été repris en 2005 (2) et en 2007 (3) par les diverses chambres de la Cour de cassation. En cause, l'un des cocontractants a commis une **erreur par défaut de curiosité** lors de la conclusion du contrat qui lui a fait ignorer une **information déterminante**, connue du prestataire qui l'a intentionnellement **dissimulée**.
- La question de l'**obligation précontractuelle d'information** entre les parties est une problématique récurrente dans les contrats informatiques qui est souvent la source de contentieux (4).
- Si depuis longtemps la jurisprudence a reconnu le déséquilibre informationnel existant entre un **professionnel** et son **client profane**, elle n'a pas pour autant exclut tout devoir d'information à la charge de ce dernier.
- En matière informatique non seulement le client doit **définir ses besoins** mais il doit **se renseigner** sur le produit où le service pour lequel il contracte. Dans le cas contraire cela pourrait lui être reproché si un désaccord l'oppose au prestataire et abouti à l'échec du projet. Encore faut-il qu'il sache sur quoi se renseigner.
- La principale source d'information du client étant son prestataire, il n'y a en principe aucune raison pour qu'il mette en doute les informations communiquées. C'est là toute la portée de cette jurisprudence en matière informatique, le **client s'en remet** naturellement **à l'expertise du prestataire** qui peut donc facilement le **tromper** ne serait-ce qu'en lui dissimulant une partie des informations.
- Dès lors, s'il a intentionnellement dissimulé une information déterminante, quand bien même aurait-elle été accessible au client par un autre biais, la **négligence du client** doit être couverte par la tromperie du prestataire.

Eléments constitutifs du dol dans les contrats informatiques

- Le prestataire en tant que professionnel de l'informatique est soumis à une **obligation d'information et de conseil renforcée**.
- Quand bien même le client aurait commis une erreur en **ne se renseignant pas** suffisamment, si le prestataire informatique a intentionnellement dissimulé à son client des informations éclairantes de son consentement, alors l'**erreur** est nécessairement **excusable**.
- Pour qualifier le **dol par réticence** le client doit rapporter la preuve de :

- l'existence de l'information,
- l'intention de ne pas la divulguer
- son caractère déterminant du consentement.

- Cette **triple preuve** reste extrêmement difficile à rapporter en matière informatiques dès lors qu'elle ressortira la plupart du temps de points techniques dont le tribunal pourra difficilement apprécier l'importance.

L'enjeux

La réticence dolosive rend toujours excusable l'erreur de la victime.

Le défaut de curiosité du client est couvert par l'intention dolosive du prestataire.

(1) Cass, civ 3e, 21-2-2001 n°98-20817.
(2) Cass, civ. 1e 18-1-2005 n°03-15115.
(3) Cass, com. 13-2-2007 n°04-16520.
(4) Cf. Alain Bensoussan, «Informatique, Télécoms, Internet », Ed. Francis Lefebvre, 5e éd. 2012, nos 451 et s.

Les conseils

Prévoir une clause :
- affirmant que le prestataire a fourni toutes les informations nécessaires aux besoins formulés par le client
- rappelant l'expertise informatique du client ou de l'assistance reçue d'un tiers spécialiste durant les négociations

BENOIT DE ROQUEFEUIL
ARNAUD MARC

RUPTURE BRUTALE DES RELATIONS COMMERCIALES DU FAIT DU CHANGEMENT DE DIRIGEANTS

L'autonomie de la personne morale et l'intuitu personae

▪ Un fournisseur a rompu les relations contractuelles avec son distributeur apprenant que celui-ci avait cédé toutes ses parts entraînant un changement de dirigeant social.

▪ Considérant que cette **résiliation** était **brusque et fautive**, le distributeur l'a assigné en paiement de dommages et intérêts sur le fondement de la rupture brutale des relations commerciales établies.

▪ La Cour d'appel de Montpellier a considéré que le **changement de dirigeant** de la société et la cession du capital ne constituaient pas une faute du distributeur et **ne justifiaient pas la résiliation** du contrat par le fournisseur.

▪ Le fournisseur a formé un pourvoi contre cette décision au motif que le contrat de distribution était un **contrat conclu *intuitu personae*** et qu'en conséquence, la rupture ne pouvait être qualifié d'abusive. La Cour de cassation a **rejeté le pourvoi** :

- « *en raison du principe d'autonomie de la personne morale, cette dernière reste inchangée en cas de cession de la totalité des parts ou actions d'une société ou de changement de ses dirigeants* » et de
- « *l'absence de stipulation contractuelle* [autorisait] *la rupture avant échéance dans de telles hypothèses* ».

▪ Elle a **approuvé** la décision de **la Cour d'appel de Montpellier** en ce qu'elle a, *« sans écarter le caractère intuitu personae du contrat »* déduit à bon droit que *« en l'absence d'une stipulation particulière, la convention était maintenue en dépit des changements survenus* ».

▪ En outre, elle a ajouté que « *la période de cinq mois correspondant au maintien effectif et provisoire de la relation commerciale établie devait être imputée sur le délai de préavis jugé nécessaire* ».

Attention à la rupture brutale des relations commerciales

▪ Cette décision réaffirme le principe de l'**autonomie de la personne morale**.

▪ Ainsi, sans remettre en cause le caractère *intuitu personae* du contrat, la Cour de cassation énonce l'interdiction, en l'absence de stipulations contractuelles contraires, de prendre en compte le changement de dirigeant.

▪ En réalité cela peut se comprendre de la façon suivante : le caractère ***intuitu personae*** est **attaché à la personne morale** elle-même et non à la personne physique représentant la personne morale.

▪ Les conventions passées entre les parties sont donc maintenues et ce, en dépit d'éventuels changements de dirigeant.

▪ Concernant le **délai de préavis** considéré comme suffisant au regard de la durée des relations commerciales, la Cour de cassation rappelle le principe selon lequel « *l'adéquation du préavis écrit qui est consenti, tenant compte de la durée de la relation commerciale, s'apprécie à la date à laquelle l'auteur de la rupture notifie son intention d'y mettre fin* ».

Les enjeux

Si aucune stipulation contractuelle n'autorise la rupture avant échéance dans l'hypothèse d'un changement de dirigeant, le contrat doit être maintenu.

La rupture du contrat entraîne l'obligation de réparation de la faute constituée par la rupture brutale du contrat.

(1) Cass. com. 29-1-2013 n°11-23676.

Les conseils

- prévoir une clause précisant le caractère *intuitu personae* du contrat, le cas échéant.
- en cas de changement de dirigeant, procéder à un état des lieux des contrats pour identifier de telles clauses.

MARIE-ADELAÏDE DE MONTLIVAULT-JACQUOT
ALEXANDRA MASSAUX

METTRE EN PLACE UNE POLITIQUE DE SECURITE CONTRE LES ATTAQUES CIBLEES

Les PME représentent le chemin d'accès le moins résistant

Les enjeux

- Cyber espionnage, logiciels malveillants, phishing, rançongiciels, maliciels sur mobile et sites web malveillants, selon le Symantec, le nombre d'attaques ciblées a augmenté de **42 %** dans le monde **entre 2011 et 2012** (1).
- Si la **France** se classe au 16e rang mondial des **pays les plus actifs** en matière de cybercriminalité, elle est aussi placée parmi les **pays les plus vulnérables** aux attaques ciblant les réseaux. Elle occupe le 10e au niveau mondial et le 5e au niveau européen.
- En revanche, on note un fort **recul du spam**, puisque la France se place 42e dans le monde et 17e en Europe dans ce domaine.
- Aucune taille d'organisation n'est épargnée, les **sous-traitants** offrant souvent des portes d'entrées aisées vers de plus grosses entreprises en utilisant la technique du « **watering hole** » (trou d'eau ou abreuvoir).
- Il s'agit d'une **technique d'attaque** consistant pour les hackers, à identifier les hobbies des cadres ou grands patrons de société, puis à les attendre patiemment sur un site référent en la matière que l'on a compromis pour les infecter lorsqu'ils s'y rendent.
- En 2012, 50 % des attaques ciblées ont visé des entreprises de moins de 2500 salariés. 31 % des attaques ont concerné des entreprises de moins de 250 salariés, une multiplication par 3 par rapport à 2011.
- Le niveau de sophistication des attaques, qui va de pair avec la complexité croissante des infrastructures informatiques actuelles, tels que la virtualisation, la mobilité et le cloud computing.

Chaque année, le rapport « Internet Security Threat Report » (ISTR) l'éditeur de logiciels anti-virus Symantec dresse un aperçu des menaces observées au niveau mondial.

(1) 18e rapport annuel Symantec, avril 2013.

Avoir une politique de sécurité contre les menaces informatiques

Les conseils

- L'Agence nationale de la sécurité des systèmes d'information (**ANSSI**) met en garde les entreprises contre toutes les **menaces pesant sur les sites :** défigurations, dénis de service ou scénarios d'attaques plus insidieux permettant de se servir d'un site comme une porte d'entrée vers le système d'information.
- L'Agence a émis des **recommandations** en **avril 2013** rappelant que la protection passe à la fois par des **mesures préventives** et par des mécanismes permettant de détecter les tentatives d'attaques (2).
- De même, l'ANSSI a émis des recommandations en **mai 2013** sur les risques liés à l'usage de plus en plus répandu des « ordiphones » (**smartphones**) ou des tablettes en environnement professionnel.
- Ces terminaux qui disposent de nombreuses fonctionnalités rendent possible la connexion à un réseau d'entreprise pour travailler sur des applications métier ou **accéder à des documents professionnels**.
- Or les **solutions de sécurisation** actuelles sont peu efficaces pour assurer une protection correcte des données professionnelles (3).
- Enfin, l'ANSSI a publié en **janvier 2013**, la version finalisée du guide d'hygiène informatique à destination des entreprises. Ce document présente 40 recommandations simples pour sécuriser leur(s) système(s) d'information.

Un petit-déjeuner est organisé au cabinet le 19 juin 2013 analysera les nouveaux risques TIC et leur assurabilité.

(2) Recom. ANSSI n°DAT-NT-009/ANSSI/ SDE/NP du 22-4-2013.
(3) Recom. ANSSI n°DAT-NT-010/ANSSI/ SDE/NP du 15-5-2013.

JEAN-FRANÇOIS FORGERON
ISABELLE POTTIER

DROIT DES MARQUES : LES MODIFICATIONS A VENIR DU DROIT EN VIGUEUR

La réforme du droit des marques proposée par la Commission européenne

▪ Le 27 mars 2013 la Commission européenne a présenté une **réforme du droit des marques** en vigueur sur le territoire de l'Union européenne (1) après avoir mené de nombreuses consultations, dont le fameux rapport de l'Institut Max Planck pour la Propriété Intellectuelle et le Droit de la Concurrence.

▪ Les **objectifs** annoncés sont de **faciliter l'accès** aux marques en rendant les systèmes d'enregistrement de marques moins chers, plus rapides, plus fiables et plus prévisibles sur l'ensemble de l'Union européenne ainsi que d'**améliorer la protection** conférée par les marques notamment à l'égard des produits contrefaisants en régime de transit sur le territoire de l'Union européenne.

▪ La Commission européenne propose quatre grands **axes de réforme** : la **rationalisation** et l'**harmonisation** des procédures d'enregistrement des marques à l'aune du système de la marque communautaire, la **modernisation de la législation** en vigueur (suppression des dispositions obsolètes et intégration des principes dégagés par la jurisprudence du Tribunal de l'UE et de la Cour de l'UE, le **renforcement des moyens de luttes** contre les marchandises contrefaisantes en transit sur le territoire européen et enfin l'accroissement de la **coopération** entre les offices des Etats membres et l'Office de l'harmonisation dans le Marché Intérieur (OHMI) pour créer des pratiques convergentes et des **outils communs**.

▪ Elle préconise en revanche le **maintien de la coexistence** de deux systèmes de protection de marque sur le territoire européen : les **marques nationales** protégées dans chacun des Etats et la **marque communautaire** protégée dans toute l'UE.

Harmonisation et protection renforcées

▪ Parmi les propositions de modification portant sur la directive d'harmonisation des législations sur les marques (2), le règlement sur la marque communautaire (3) et celui sur les taxes à payer à l'OHMI pour la marque communautaire, on retient une **modification de la définition de la marque** qui ne serait plus nécessairement un signe susceptible de représentation graphique et permettrait de réintroduire la possibilité de protéger les signes olfactifs à titre de marque.

▪ L'harmonisation des procédures d'enregistrement et de la protection des marques collectives et des marques de renommée est envisagée. En outre, la protection des **noms géographiques protégés** serait renforcée.

▪ Les indications géographiques, mentions traditionnelles pour les vins et spécialités traditionnelles garanties devraient constituer des droits opposables aux marques pour toutes les législations au sein de l'Union.

▪ Par ailleurs, les procédures de déchéance ou de nullité des marques nationales pourraient être désormais introduites devant les offices de propriété industrielle (4).

▪ Il est aussi prévu la possibilité pour les titulaires de droits d'empêcher des tiers d'introduire sur le territoire douanier de l'Union des produits, qu'ils aient ou non été mis en libre pratique, provenant de pays tiers et portant sans autorisation une marque pratiquement identique à celle déjà enregistrée pour ces produits. Enfin, sous certaines conditions, constituerait un **acte de contrefaçon** l'usage, en tant que nom commercial, d'une marque protégée.

Les enjeux

Anticiper les réformes du droit des marques.

(1) Communiqué IP-13-287, Bruxelles le 27-3-2013.
(2) Proposition directive, Com(2013) 162 final, Bruxelles le 27-3-2013.
(3) Proposition de règlement, COM(2013) 161 final, Bruxelles le 27-3-2013.
(4) En France, ces actions ne peuvent être introduites que devant les dix tribunaux de grande instance compétents Tableau VI annexé au Code de l'organisation judiciaire.

Les conseils

Suivre le processus de codécision entre le Parlement européen et le Conseil en vue d'anticiper les réformes.

ANNE-SOPHIE CANTREAU
JULIE FEUVRIER-LAFORET

LES NANOMATERIAUX : QUELLES INCIDENCES SUR LA SANTE ET SUR L'ENVIRONNEMENT ?

Les nanomatériaux manufacturés sont présents dans la vie quotidienne

▪ Les nanomatériaux manufacturés, donc produits et introduits délibérément dans l'environnement par l'homme, sont aujourd'hui intégrés dans la composition de nombreux produits utilisés dans la **vie courante** (produits cosmétiques, textiles, alimentaires, etc.).

▪ Les nanomatériaux sont utilisés dans des secteurs aussi divers que l'**automobile**, la **chimie**, l'**énergie**, l'**environnement** et la **santé**.

▪ Les nanomatériaux manufacturés sont constitués de structures élémentaires dont au moins une des dimensions est comprise typiquement, mais non exclusivement, entre **1 et 100 nanomètres** (nm), millionième de millimètre.

▪ Cette caractéristique dimensionnelle confère aux matériaux des propriétés ou des comportements particuliers, utilisés pour de **nouvelles applications technologiques**.

▪ La **toxicité potentielle** associée aux nanomatériaux est dépendante de leurs propriétés physico-chimiques (taille, caractère soluble, surface spécifique, état de surface ou forme du nano-objet), chaque nanomatériaux pouvant réagir différemment en fonction de la formulation et la matrice du produit fini qui le contient.

▪ En raison de ces spécificités, les connaissances scientifiques sur les substances classiques ne sont pas directement transposables aux formes nanométriques.

▪ Les **incertitudes** sur l'évaluation quantitative des risques et menaces ne seront levées qu'au fur et à mesure de la progression des **connaissances scientifiques** des propriétés des nanomatériaux manufacturés.

▪ En outre, il n'existe **pas de méthode standardisée** permettant de mesurer et de suivre le devenir de nanoparticules manufacturées dans des matrices complexes (environnement, aliments, organisme).

L'obligation de déclaration

▪ Les industriels ont, **depuis le 1er janvier 2013**, l'obligation de déclarer les nanomatériaux, conformément à la réglementation en vigueur sur l'application de déclaration en ligne des substances à l'état nanoparticulaire « r-nano » (1).

▪ L'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (**ANSES**) est chargée de la gestion des déclarations et des données, les premières informations issues des déclarations seront mises à la disposition du public par cette dernière d'ici la fin de l'année 2013 conformément aux dispositions de l'article L. 521-7 du Code de l'environnement.

▪ Selon l'ANSES, à l'échéance du 30 avril 2013, **457 entreprises** ont réalisé **1991 déclarations**, ce qui démontre une mobilisation jugée satisfaisante des acteurs visés par l'obligation de déclaration.

▪ Le Ministère de l'Écologie, du Développement Durable et de l'Énergie, a récemment pris en compte la diversité des acteurs visés par l'obligation de déclaration, ainsi que la demande de plusieurs secteurs d'activité et a décidé, pour cette première année de déclaration, d'accorder **2 mois supplémentaires** pour effectuer leur déclaration. De nouvelles déclarations pourront donc être initiées et soumises jusqu'au 30 juin 2013.

Les enjeux

Encadrer l'utilisation des nanomatériaux manufacturés qui sont présents dans la vie quotidienne par une obligation de déclaration afin de disposer d'une traçabilité des filières d'utilisation.

Les connaissances actuelles et disponibles sur la toxicité des nanomatériaux manufacturés sont encore aujourd'hui lacunaires.

(1) Décret 2012-232 du 17-2-2012 et arrêté du 6-8-2012.

L'essentiel

Un petit-déjeuner est organisé au cabinet le 26 juin 2013 pour permettre aux acteurs visés par l'obligation de déclaration de disposer d'un premier bilan à mi-chemin avant la date butoir de fin de déclaration.

DIDIER GAZAGNE

NOUVELLES EXTENSIONS GTLDS : LES INDICATIONS GEOGRAPHIQUES EN DANGER

Les GTLDs géographiques… éléments fort de la valorisation d'un produit

▪ La **Confédération Nationale des producteurs de vins et eaux de vie de vin à Appellations d'Origine Contrôlées** (CNAOC) et l'**European Federation of Origin Wines** (EFOW) interpellent l'opinion publique sur le dépôt de quatre dossiers de candidature d'extensions génériques de noms de domaines comportant le « **.vin** » (1 dossier) et le « **.wine** » (3 dossiers en concurrence).

▪ Elles craignent que les sociétés qui seront sélectionnées par l'ICANN soient « en mesure de commercialiser ces noms de domaine permettant ainsi à des individus et/ou à des organisations de les combiner à un nom de domaine de second niveau pour créer une adresse Web personnalisée telle que "chianti.wine", "champagne.vin", "rioja.wine", "port.wine" et bien d'autres » sans aucun droit sur l'appellation d'origine ou les indications géographiques protégées (1).

▪ Il est rappelé qu'en juin 2011, l'ICANN avait approuvé le programme de lancement de nouvelles extensions génériques (**gTLDs**) de noms de domaine. Les candidatures ont pu être déposées entre le 12 janvier et le 29 mars 2012. Au total, 1930 candidatures ont été reçues par l'ICANN.

▪ Le 31 mai 2013, l'ICANN annonçait que **514 candidatures** avaient passé le stade de l'**évaluation initiale** qui est une étape du processus de **délégation**, la finalisation de l'évaluation initiale ne signifiant pas automatiquement que les extensions seront déléguées, certaines pouvant ensuite échouer au stade d'une évaluation approfondie, d'une procédure d'objections ou de résolution de conflits avec d'autres candidatures (2).

…au cœur de vives polémiques

▪ L'enjeu majeur est d'attirer l'attention de **l'ICANN** sur la protection des indications géographiques dans le monde **Internet**, à l'instar de la protection déjà prévue par les traités internationaux et par les législations nationales, de sorte que ces premières ne puissent pas être administrées par des tiers indélicats qui seraient tentés ensuite de les céder à des prix prohibitifs aux représentants et acteurs économiques du secteur ou encore qui profiteraient sciemment de leur incontestable **notoriété** pour engendrer une **confusion** dans l'esprit des **consommateurs**.

▪ Les appellations d'origine ne sont pas les seules touchées par l'attribution de ces nouvelles extensions de noms de domaine. En effet, le Brésil et le Pérou s'insurgent également contre la demande d'attribution du « .amazon » au bénéfice de la célèbre société éponyme (3).

▪ S'il est vrai que ces nouvelles extensions ouvrent de sérieuses perspectives pour renforcer une présence et une **identité sur Internet**, leur délégation ne doit pas être réalisée au détriment d'intérêts collectifs privés ou publics. La prochaine session de l'ICANN, à Durban en Afrique du Sud en juillet prochain, devrait apporter des éléments nouveaux sur ces dossiers épineux.

Les enjeux

Les indications géographiques ont toujours attiré les convoitises. Il suffit pourtant d'évoquer les célèbres affaires concernant l'usage de l'appellation d'origine contrôlée « champagne » pour désigner des tabacs ou un parfum pour savoir que les confédérations et syndicats sont très attentifs aux tentatives d'appropriation par les tiers non autorisés (Cass. com. 18-02-2004 ; TGI Paris 5-3-1984).

Les conseils

Surveiller les nouvelles candidatures.

(1) CNAOC actualité du 26-4-2013.
(2) Guide de candidature gTLD, Version 19-9-2011.
(3) GAC Early Warning-Submittal, Amazon-BR--PE-58086.

CLAUDINE SALOMON
ANNE-SOPHIE CANTREAU

LE NATIVE ADVERTISING OU LE PUBLI-REDACTIONNEL DIGITAL

Le native advertising, une publicité de qualité à destination du consommateur

L'enjeu

▪ Le native advertising est annoncé comme la nouvelle tendance marketing et fait à ce titre le buzz dans la communauté marketing.

▪ Il apparaît comme un **nouveau format publicitaire**, en réaction aux formes traditionnelles de publicité sur le net en particulier bannières, pop-up, jugées comme trop intrusives. Le native advertising fonctionne selon le triptyque suivant :

- un contenu ;
- un message publicitaire inséré dans un contenu ;
- un message ciblé et adapté au contexte du contenu.

Délivrer un message de qualité pour compléter les informations fournies aux consommateurs.

Améliorer leur expérience et les replacer au centre de la relation annonceur/éditeur.

▪ Plusieurs géants du web s'y sont mis dont Yahoo qui a dévoilé fin avril son tout nouveau format publicitaire baptisé "*Yahoo Stream Ads*", **posts sponsorisés** intégrés dans la homepage de ses versions ordinateur, tablette et mobile (1).

▪ Le native advertising consiste à mettre à disposition des consommateurs du **contenu éditorial** de qualité, ce qui le rapproche du **publi-rédactionnel** traditionnel. Comme lui, il est une publicité intégrée dans un espace publicitaire d'un support.

(1) PC INpact, le 30-4-2013.

Le native advertising, une publicité en toute transparence

Les conseils

▪ Selon l'Autorité de régulation professionnelle de la publicité (ARPP), lorsqu'une publicité est diffusée dans des médias qui comportent également des informations ou des articles rédactionnels, elle doit être présentée de telle sorte que son **caractère publicitaire apparaisse instantanément** (2).

Faire apparaitre de manière claire et lisible le caractère publicitaire du message

▪ Il est d'ailleurs fait obligation aux annonceurs, agences et supports de presse de faire figurer les mots **publicité** ou **communiqué** d'une manière claire et lisible en tête de toute annonce présentant les caractéristiques d'une **publicité rédactionnelle**, si cette annonce est payée.

▪ Concernant la **communication publicitaire digitale**, l'ARPP précise également qu'il « *est alors recommandé d'adjoindre une indication explicite permettant d'identifier la publicité comme telle " et lorsque " le message est diffusé au milieu d'informations ou d'articles rédactionnels, qu'il doit être présenté de manière à ce que son caractère publicitaire apparaisse instantanément* » (3).

Etre transparent, loyal et identifiable

▪ Cette **indication** doit être **lisible** ou **audible** et **intelligible**.

▪ De plus, l'annonceur doit être aisément identifiable. Cette identification doit être clairement perceptible et facile d'accès pour le public. Sur ce point, l'ARPP précise que « *l'identification peut se faire par la/les marque(s) de l'annonceur, ou tout autre signe distinctif rattaché sans ambiguïté à l'annonceur* ».

(2) Recommandation Identification de la publicité, ARPP oct. 2008.

(3) Communication publicitaire digitale, ARPP déc. 2010.

▪ Si le native advertising a le vent en poupe et est la **tendance marketing** actuelle, son salut passera par une **identification du message** comme toute publicité pour ne pas tromper le consommateur, dans la mesure où les premières études ont démontrées que l'affichage de la **nature réelle du message** est un facteur de confiance.

CELINE AVIGNON
ANNE RENARD

L'INTERDICTION DE RECOURIR A UNE MARQUE DANS UN MARCHE PUBLIC N'EST PAS ABSOLUE

La référence à des marques dans un marché public

▪ L'article 6 du Code des marchés publics dispose que « *Les spécifications techniques ne peuvent pas faire mention d'un mode ou procédé de fabrication particulier ou d'une provenance ou origine déterminée, ni faire référence à une marque, à un brevet ou à un type, dès lors qu'une telle mention ou référence aurait pour effet de* ***favoriser*** *ou d'****éliminer*** *certains opérateurs économiques ou certains produits. Toutefois, une telle mention ou référence est possible si elle est* ***justifiée*** *par l'objet du marché ou, à titre* ***exceptionnel****, dans le cas où une description suffisamment précise et intelligible de l'objet du marché n'est pas possible sans elle et à la condition qu'elle soit accompagnée des termes ou équivalent* ».

▪ Par ailleurs, le décret fixant le statut de la normalisation (1) prévoit que « *Les clauses, spécifications techniques et cahiers des charges des marchés et contrats visés par le décret ne peuvent mentionner des produits d'une* ***fabrication*** *ou d'une* ***provenance déterminée****, ou des procédés particuliers à certaines entreprises. Ils ne peuvent pas plus contenir de références à des brevets, à des indications d'origine ou de provenance, à des marques telles qu'elles découlent ;* ***sauf*** *lorsqu'il n'est pas possible de donner une description de l'objet du marché ou du contrat sans ces références. Dans ce dernier cas, de telles références sont autorisées si elles sont accompagnées de la* ***mention*** *"****ou équivalent****"* ».

▪ Il ressort de ces textes qu'une marque ne peut être citée que dans le seul cas où cette référence permet de décrire l'objet du marché ou du contrat.

La référence à une marque justifiée par l'objet du marché de services

▪ Une université a lancé en avril 2009, une **consultation** pour l'attribution, selon une **procédure adaptée**, d'un marché de fourniture et mise en œuvre d'un **progiciel** de gestion de salles, des emplois du temps et des ressources de l'université.

▪ Une société évincée, suite au **rejet de sa demande d'annulation** du marché par le tribunal administratif de Poitiers en mai 2011, a fait appel de la décision devant la **Cour administrative d'appel de Bordeaux** qui a **confirmé** le jugement critiqué.

▪ Dans son arrêt en date du **14 février 2013** (2), la Cour administrative d'appel de Bordeaux a constaté que « *l'article 4.2 du cahier des clauses techniques particulières prévoit que l'application devra s'appuyer sur le système de gestion de bases de données relationnelles Oracle* ».

▪ Elle a ensuite estimé que « *si la société requérante soutient que la référence à une marque est interdite, il ressort des pièces du dossier que* ***toutes les applications métiers de l'université de Poitiers utilisent le système Oracle****, que ce dernier permet des facilités de liaisons-interfaces avec l'entrepôt de données et que son coût est nul pour l'université* ».

▪ En l'espèce, il ne s'agissait pas de citer une **marque** en tant qu'exigence d'un produit de la marque donnée mais uniquement **en termes d'existant** sur lequel l'opérateur économique devait s'appuyer compte tenu des investissements initiaux de l'Université. Le tribunal en a déduit que « *l'université de Poitiers a pu régulièrement exiger que l'application proposée s'appuie sur le* ***système Oracle*** ».

Les enjeux

Les dérogations prévues au principe d'interdiction sont très restrictives. Le non-respect du principe constitue pour le pouvoir adjudicateur un manquement aux obligations de publicité et de mise en concurrence susceptible d'entrainer l'annulation du marché.

(1) Décr. n°84-74 du 26-1-1984 modifié.
(2) CAA Bordeaux, 14-2-2013 n°11BX01785 Société Index Education/ Université de Poitiers.

Les conseils

Il appartient au pouvoir adjudicateur qui souhaite imposer aux candidats du marché le recours à une marque, de détailler avec précisions dans l'objet du marché les motifs justifiant l'utilisation de cette référence.

Il devra établir que la réalisation du marché ne peut être possible sans faire appel à la marque en cause ou que les produits de cette dernière sont les seuls à répondre à ses besoins.

FRANÇOIS JOUANNEAU
MAGALI GRANIER

LIBERALISATION DES DISPOSITIFS TECHNIQUES DE DEMATERIALISATION DES FACTURES

Renforcement des caractéristiques de la signature électronique

Les enjeux

▪ La **loi de finances rectificative pour 2012** (1) a transposé en droit interne (2) certaines dispositions de la directive 2010/45/UE du Conseil du 13 juillet 2010.

▪ Outre l'**égalité de traitement** entre les factures **papier** et les factures **électroniques**, cette directive reconnait la possibilité aux assujettis à la taxe sur la valeur ajoutée (TVA) d'émettre et de recevoir des factures électroniques en recourant à **n'importe quel dispositif technique** sous certaines conditions.

A compter du 1er janvier 2013, les factures électroniques peuvent être émises et reçues sous une forme électronique quelle qu'elle soit.

▪ Il faut que des **contrôles fiables** soit mis en place afin d'établir le lien entre les factures émises ou reçues et la livraison de biens ou la prestation de services qui en est le fondement.

▪ Les conditions d'application de ces nouvelles dispositions ont été précisées par le **décret du 25 avril 2013** (3) qui a modifié en conséquence les dispositions de l'annexe III au Code général des impôts.

▪ Les dispositifs de dématérialisation des factures électroniques jusqu'alors en vigueur (signature électronique et échange de données informatisées) sont maintenus.

▪ Le décret **renforce** toutefois les **caractéristiques de la signature électronique** qui doit désormais être fondée sur un certificat électronique qualifié et être créé par un dispositif sécurisé de création de signature électronique.

(1) Loi 2012-1510 du 29-12-2012, art. 62.

(2) CGI, art. 289 VII.

(3) Décr. 2013-350 du 25-4-2013.

(4) CGI, art. 96 F, 96 F bis, 96 G, 96 H, 96 I, 96 I bis de l'annexe III.

Codification des règles d'échange de données informatisées

Les conseils

▪ Le décret procède également à la **codification** des dispositions relatives à l'échange de données informatisées.

▪ Il précise que les entreprises qui utilisent ce dispositif pour leur facture électronique doivent recourir à un système de télétransmission répondant aux **normes définies par la Commission européenne** concernant les aspects juridiques de l'échange de données informatisées, lorsque l'accord relatif à cet échange prévoit l'utilisation de procédés garantissant l'**authenticité** de l'origine et l'**intégrité** des données.

Le dispositif technique choisi exige toutefois la mise en place de contrôle fiable entre la facture émise ou reçue et la livraison de biens ou la prestation de services qui en est le fondement.

▪ Les autres dispositions de ce décret précisent les **modalités de conservation** des factures dont l'authenticité de l'origine, l'intégrité du contenu et la lisibilité des factures doivent être assurées par les contrôles mis en place par les assujettis.

▪ Il précise également les règles applicables en matière de **restitution des factures**, sous forme papier ou électronique.

PIERRE-YVES FAGOT

ACTUALITES

Autorisation administrative et licenciement d'un salarié protégé

▪ La Cour de cassation vient de rappeler que le statut protecteur de **représentant du personnel** empêche toute action de l'employeur qui anticiperait sur la fin proche de la protection (1). Il ne peut, au motif que le salarié protégé ne bénéficiera plus de son statut dans quelques jours, s'exonérer de la **consultation obligatoire de l'inspection du travail**, qui ne sera plus « compétent » au moment de rendre sa décision.

▪ C'est la **date de l'envoi** et non celle de la réception de la convocation à l'entretien préalable au licenciement qui compte.

▪ La Cour, dans ce même arrêt réaffirme le **droit à réintégration du salarié** (encore bénéficiaire du statut protecteur) abusivement licencié alors même que cette protection est arrivée à expiration.

▪ En revanche, **l'indemnisation corrélative** à sa demande de réintégration, si elle est exigible, doit être **limitée** dans son montant au regard du délai que le salarié a laissé courir après l'expiration de la période de protection.

▪ En l'espèce, le salarié avait attendu 4 ans après l'expiration de ladite période pour en faire la demande, ce que la Cour a jugé abusif ; il en a résulté que celle-ci ne lui a pas octroyé la totalité du montant demandé.

▪ Il convient de noter par ailleurs que l'indemnisation d'une clause de non concurrence illicite (parce que ne prévoyant pas de contrepartie financière) n'est pas due au salarié protégé qui demande sa réintégration.

L'enjeux

L'employeur est tenu de demander l'autorisation administrative de licencier un salarié lorsque ce dernier bénéficie du statut protecteur à la date de l'envoi de la convocation à l'entretien préalable au licenciement.

Peu importe que le courrier prononçant le licenciement soit envoyé postérieurement à l'expiration de la période de protection.

(1) Cass. soc. 26-3-2013, n°11-27964.

Télétravail et développement des tiers lieux

▪ Le Cabinet Greenworking vient de publier les résultats d'une **étude commandée** par le Ministre de l'Industrie, de l'Energie et de l'Economie numérique et réalisée auprès d'une vingtaine de grandes entreprises françaises pratiquant le télétravail.

▪ L'**objectif** de l'étude est d'analyser les principaux enseignements tirés de la pratique du télétravail dans ces entreprises et de mettre en lumière les **perspectives de développement** de ce mode de travail pour l'avenir.

▪ Il ressort de l'étude que l'**usage modéré** du télétravail (30% du temps de travail d'un salarié), favorise une optimisation des conditions de travail et une productivité accrue ; et ce, d'autant plus lorsque le télétravail est réalisé dans un " **tiers lieu** ", permettant le maintien de la distinction entre sphère personnelle et professionnelle. Selon cette étude, la **réussite** de la mise en œuvre du télétravail repose sur :

▪ La combinaison d'un processus exigeant information et **sensibilisation** en amont ;

▪ la **reconnaissance** du télétravail comme mode de travail à part entière ;

▪ la mise en place d'une **démarche progressive** (temps d'adaptation) ;

▪ l'investissement dans des **outils fiables** et innovants et infrastructures de qualités ;

▪ l'**accompagnement** du projet par une adéquation des pratiques managériales ;

▪ la **formation** de toutes les parties prenantes ;

▪ le **retour sur expériences** et la proposition de solutions aux pratiques déviantes;

▪ et enfin la mise en place d'un **dispositif de suivi** et d'évaluation des impacts afin de piloter le projet et d'assurer une adhésion de la gouvernance de l'entreprise.

Les conseils

Au-delà des aménagements techniques et juridiques nécessaires, c'est l'adhésion, facteur culturel pivot, qui permettra un réel développement du télétravail.

(2) Conclusions de l'étude sur le télétravail lancée par le Ministre de l'Industrie, M. Eric Besson, 30-4-2013.

EMMANUEL WALLE
NAOMI SUCHOD

Prochains événements

Entre la médiation et les actions de groupe : quelle marge de manœuvre ? : 5 juin 2013

▪ Annie Gautheron-Vebret, animera aux côtés de **Frank Thomelin,** médiateur chez Esprit Médiation un petit-déjeuner débat consacré au projet de loi sur la médiation et les actions de groupe.
▪ Mesure phare du projet de loi sur la médiation présenté au conseil des ministres du 2 mai dernier, l'action de groupe suscite dans ce contexte de légitimes réactions sur le principe de son introduction dans le droit français, et de sérieuses interrogations sur ses spécificités par rapport à la class action à l'américaine. Il est essentiel de déterminer l'étendue de la marge de manœuvre que le recours à la médiation laisse aux parties lorsque leur conflit relève de l'action de groupe telle qu'envisagée par le projet de loi :
• Quelles sont les spécificités du projet d'action de groupe à la française ?
• Quelles en seraient les conséquences pour l'entreprise poursuivie ?
• La médiation peut-elle jouer son rôle de mode alternatif de règlement des litiges ?
▪ **Inscription gratuite** sous réserve de confirmation avant le 3 juin 2013 par formulaire d'inscription en ligne.

Les nouveaux risques TIC : quelle assurabilité ? : 19 juin 2013

▪ Jean-François Forgeron animera aux côtés de **Nicolas Hélénon**, Neotech Assurances (groupe LSN) un petit-déjeuner débat consacré aux nouveaux risques TIC : quelle assurabilité ?
▪ Du piratage informatique, aux virus, en passant par la perte de données, quels sont les menaces informatiques assurables ? Le nombre d'attaques ciblées visant les entreprises a été multiplié par trois entre 2011 et 2012 (18e édition du rapport annuel de la société Symantec publié en avril 2013). Aucune taille d'organisation n'est épargnée, les sous-traitants offrant des portes d'entrées aisées vers de plus grosses entreprises.
▪ Une politique de sécurité ne peut garantir contre toutes les menaces informatiques. Aucun réseau n'est à l'abri d'une faille sécuritaire. Avec le futur règlement européen sur la protection des données, la notification des failles deviendra une obligation à l'égard des clients en cas d'atteinte à leurs données informatiques.
• Quelles sont les menaces informatiques assurables ?
• Peut-on couvrir les frais de notification (Data Risks Protection) ? d'atteinte à la réputation ?
• Comment estimer ce que vaut réellement une donnée ? (coût pour remédier à un data breach)
• L'externalisation en mode cloud change-t-elle l'analyse du risque des entreprises clientes de ce type de services ?
• Quels sont les audits de sécurité du SI à mener ? (tests d'intrusion, droits d'accès, etc.)
• Telles seront les questions qui seront débattues lors de ce petit-déjeuner.
▪ **Inscription gratuite** sous réserve de confirmation avant le 17 juin 2013 par formulaire d'inscription en ligne.

Nanomatériaux : quels enjeux et responsabilités pour les industriels ? : 26 juin 2013

▪ Alain Bensoussan et Didier Gazagne animeront aux côtés de **Thomas Nappez** co-fondateur de NanoThinking et **Nicolas Feltin** Club NanoMétrologie LNE, un petit-déjeuner débat consacré aux Nanomatériaux : quels enjeux et responsabilités pour les industriels ?
▪ Entre innovation technologique et risques de développement, l'utilisation des nanomatériaux dans l'industrie suscite des interrogations à l'heure de la déclaration Anses. Au 30 avril 2013, 457 entreprises ont réalisé 1991 déclarations, ce qui démontre une mobilisation jugée satisfaisante des acteurs concernés. Les premières informations issues des déclarations seront mises à la disposition du public par l'Anses d'ici la fin de l'année 2013.
▪ Devant les nombreuses questions posées par les diverses situations rencontrées, le Ministère a décidé, pour cette première année, d'accorder deux mois supplémentaires pour effectuer cette démarche, soit jusqu'au 30 juin 2013.
• Que faut-il déclarer et quelles sont les informations à fournir à l'Anses ?
• Quels sont les outils métrologiques pour les nanomatériaux ?
• Quels sont les risques toxicologiques, les effets biologiques et sanitaires ?
▪ Telles seront les questions qui seront débattues lors de ce petit-déjeuner.
▪ **Inscription gratuite** sous réserve de confirmation avant le 24 juin 2013 par formulaire d'inscription en ligne.

Synthèse du petit-déjeuner du 15 mai 2013

DEPLOYER LE TELETRAVAIL : LES CLES D'UNE STRATEGIE JURIDIQUE GAGNANTE

▪ Lors du petit déjeuner débat du **15 mai 2013**, Maître **Emmanuel Walle** et **Xavier de Mazenod** ont fait un état des lieux du déploiement du télétravail par des entreprises.

▪ Le socle de base du télétravail est maintenant codifié mais il y a bien longtemps que cette pratique existe et a été encadrée par la directive communautaire transposée dans l'accord cadre de 2005. Malgré un développement de cette pratique en Europe, force est de constater qu'en France, cette pratique peine à s'implanter.

▪ Pourtant il y a très peu de contentieux relatifs au télétravail, c'est bien la preuve que son encadrement est souple et adapté. Les rares contentieux portent sur les clauses de mobilité et sur le reclassement. En outre, lorsque le télétravail est mis en place, on constate qu'il y a très peu de retour en arrière une fois intégré.

▪ Au-delà de ce constat, il convient de signaler que le télétravail n'est pas fait pour tous. Certaines activités y sont particulièrement adaptées, d'autres beaucoup moins. Il y'a des conditions d'éligibilité. En outre, tous les contextes ne sont pas adaptés. Enfin, il n'y a pas de télétravail sans confiance et une certaine autonomie.

▪ Les raisons d'y faire appel sont extrêmement variées. De la réduction des coûts (de déplacements notamment) à l'adaptation à certaines situations particulières (intempérie, grève, pandémie) en passant par l'amélioration de l'image de marque de la société ou la limitation des accidents du travail (trajet).

▪ Les vertus du télétravail s'analysent également en termes de développement durable. Pour savoir s'il s'agit d'un choix écoresponsable, il convient de prendre en compte les gains « green » (réduction du papier, émission de CO2, etc.). C'est aussi un moyen de séduire certains salariés par une meilleure organisation du travail. Du coté des salariés, les choix sont différents et correspondent davantage à une demande d'équilibre.

▪ Trois critères ont été fixés par le Code du Travail (art. L.122) pour qualifier le télétravail : il s'agit d'un travail exercé hors des locaux d'affectation, de façon régulière et répétée sur la base du volontariat, soit au domicile, soit dans des zones aménagées mutualisées. Pour mettre en œuvre un tel projet, il n'est pas obligatoire de passer par un accord d'entreprise, un avenant au contrat de travail peut suffire. Néanmoins, cela permet d'être mieux informé.

▪ Selon, la taille de l'entreprise, il sera nécessaire de consulter dans l'ordre, le CHSCT puis le Comité d'entreprise, ce dernier devant s'appuyer sur l'expertise du premier.

▪ Lorsqu'un accord cadre a été signé, il doit être fondé sur des critères objectifs (ancienneté, aptitudes à l'autonomie, partage des coûts et des responsabilités) en ce qui concerne les conditions d'éligibilité.

▪ Lorsqu'un avenant au contrat de travail est signé, il convient de faire figurer les éléments prévus dans le Code du travail (modalités du temps de travail, plage horaires de disponibilité, conditions de retour, réversibilité, descriptifs du poste, etc.). Quoiqu'il en soit, le télétravail doit être contractualisé.

▪ La charte est un outil de gouvernance particulièrement adapté aux déploiements du télétravail par sa souplesse (elle n'est pas soumise aux IRP) pour régler de nombreuses questions (confidentialité, pertes de données, usage des équipements, conformité des locaux, etc.). Elle apporte une garantie efficace de repousser les éventuels litiges issus de cette nouvelle organisation. Elle peut être utilement complétée par un guide et un livret.

▪ **Xavier de Mazenod** a présenté le Livre banc du tour de France du télétravail 2012. Il s'agit de la plus grande enquête réalisée sur le sujet. L'enquête a été menée d'octobre 2012 à mars 2013 et a permis de constater que contrairement aux idées reçues, la France n'est pas très en retard sur le déploiement de cette organisation du travail : 17 % des salariés y ont en effet recours et 73 % des français souhaitent télétravailler mais la moitié n'y parvient pas.

▪ Le premier frein à ce développement résulte d'un problème de management et non d'un problème de contrôle. Selon Xavier de Mazenod, il reste encore un important travail d'information à faire auprès des principaux acteurs.

▪ L'étude a permis de constater, par ailleurs, une explosion des lieux de co-working aménagés (tiers lieux).

▪ Si de grandes entreprises commencent à initier des projets de télétravail, beaucoup de PME y sont déjà passées mais sans l'avoir formalisé. Il ne resterait donc plus pour ces dernières qu'à régulariser certaines situations…

NOTRE RESEAU DE CORRESPONDANTS ORGANIQUES LEXING VOUS INFORME

Preuve sur Internet : l'insuffisance d'une capture d'écran

Lexing Luxembourg

Cabinet Philippe &Partners

- Prouver l'existence d'une **infraction sur Internet** peut s'avérer assez complexe. En effet, la volatilité d'Internet rend nécessaire de pouvoir figer le temps. Il est souvent recouru à cet égard aux impressions écran.
- Si, a priori, ce mode de **preuve** est admissible, encore faut-il relever qu'il est souvent bien insuffisant, surtout lorsqu'il est **contesté** par la partie adverse.
- Le Tribunal de Grande Instance de Paris a eu l'occasion de rappeler ce principe dans un jugement du **10 avril 2013**.
- Dans cette affaire mettant en scène des joueurs de rugby britanniques, le tribunal fut contraint d'écarter des pièces produites une **impression d'écran**, dès lors que l'adresse URL qui figurait en bas de page était incomplète, que l'impression d'écran ne mentionnait pas la date de sa réalisation, etc.
- La raison de cette **exclusion des preuves** réside dans la possibilité technique de modifier la page « off-line », voire d'imprimer une copie de la page litigieuse qui était présente dans la **mémoire cache de l'ordinateur**.
- Les juges reprennent l'argument du défendeur qui souligne que la page a pu être modifiée ou extraite de la mémoire cache de l'ordinateur utilisé (la preuve que cette mémoire cache ait préalablement été vidée n'étant pas rapportée).

Actualité du 7-5-2013.

Le recours électronique connaît un sérieux coup d'arrêt en Suisse

Lexing Suisse

Cabinet Sébastien Fanti.

- « En cas de transmission par voie électronique, l'observation ou non du délai se détermine non pas, comme dans les autres cas, en fonction de la date et de l'heure d'envoi, mais en fonction de la **date** et l'**heure de confirmation de la réception** de l'envoi par le système informatique de l'autorité pénale. Si la partie ne reçoit pas confirmation de la réception, elle doit mettre son pli à la poste encore dans le délai » (Cour de droit pénal, arrêt T 0/2 6B n°691/2012 du 21-2-2013).
- Cela signifie que la partie qui utilise l'électronique ne pourra guère prendre le risque d'envoyer l'écrit à minuit, voire quelques minutes avant, n'ayant pas la garantie que le système informatique répondra dans la minute ou la seconde qui suit.

Adoption à l'unanimité du projet de loi relatif au blanchiment d'argent

Lexing Maroc

Cabinet Bassamat& Associée, Fassi-FihriBassamat

- La Commission de justice, de législation et des droits de l'Homme à la Chambre des conseillers a adopté à l'unanimité, le **25 avril 2013**, le projet de loi modifiant et complétant le Code pénal et la loi de lutte contre le blanchiment de capitaux.
- Ce texte s'inscrit dans le cadre de la consécration de la volonté du Maroc d'honorer ses engagements et de poursuivre ses efforts destinés à harmoniser la législation nationale, en matière de lutte contre le blanchiment d'argent et le financement du terrorisme, avec les **normes internationales**.
- Il signe l'achèvement du plan d'action qui fait partie des engagements du Maroc vis-à-vis du **Groupe d'action financière internationale** (GAFI), depuis février 2010.

Actualité du 26-4-2013.

Recommandations de l'ANSSI pour la sécurité des « ordiphones »

▪ L'usage des ordiphones (**smartphones**) ou des tablettes est de plus en plus répandu en environnement professionnel. Ces terminaux qui disposent de nombreuses fonctionnalités rendent possible la connexion à un réseau d'entreprise pour travailler sur des applications métier ou accéder à des documents professionnels. Or les solutions de **sécurisation** actuelles sont **peu efficaces** pour assurer une protection correcte des données professionnelles. L'Agence nationale de la sécurité des systèmes d'information a émis des **recommandations** datées du **15 mai 2013** (1).

(1) Recom. ANSSI n°DAT-NT-010/ANSSI/ SDE/NP du 15-5-2013.

L'Hadopi poursuit son observation des sites de streaming

▪ L'Hadopi a dévoilé le **2 mai 2013**, son rapport relatif aux contenus présents sur la plate-forme communautaire Dailymotion (2) après avoir dévoilé en mars dernier ceux du site YouTube (3). Parmi les offres donnant accès à des biens culturels dématérialisés gratuits, Dailymotion se place seconde (derrière YouTube) en terme d'audience France parmi les sites de streaming.

(2) Qualification et quantification des contenus Dailymotion, publié le 2-5-2013.

(3) Qualification et quantification des contenus YouTube, publié en mars 2013

Recommandations de l'ANSSI pour la sécurisation des sites web

▪ Défigurations, dénis de service ou scénarios d'attaques plus insidieux permettant de se servir d'un site comme une porte d'entrée vers le système d'information, l'ANSSI met en garde contre toutes les **menaces pesant sur les sites**. La protection passe à la fois par des mesures préventives et par des mécanismes permettant de détecter les tentatives d'attaques. L'Agence nationale de la sécurité des systèmes d'information a émis des **recommandations** datées du **22 avril 2013** (4).

(4) Recom. ANSSI n°DAT-NT-009/ANSSI/ SDE/NP du 22-4-2013.

Utiliser la vidéoprotection pour verbaliser les décharges sauvages

▪ Une **proposition de loi** a été déposée le **17 avril 2013** pour étendre le champ d'utilisation de la vidéoprotection à la prévention et répression du dépôt d'immondices sur la voie publique, qui constitue une infraction au Code de l'environnement (5).

(5) Proposition de loi n° 954, déposée le 17 avril 2013.

Avertissement pour défauts de sécurité lors d'élections professionnelles

▪ La Cnil a prononcé un avertissement à l'encontre d'un grand groupe en raison de défauts de sécurité constatés lors d'élections professionnelles réalisées par vote électronique (6). Lors d'un contrôle sur place, elle a notamment constaté plusieurs **défauts de confidentialité** des données des électeurs, tels que l'envoi des identifiants et des mots de passe permettant de voter, par courrier simple ou par courrier électronique, sans procédé de sécurisation particulier.

(6) Délib. Cnil n° 2013-091 du 11-4-2013.

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 29, rue du colonel Pierre Avia 75015 Paris, président : Alain Bensoussan

Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier

Diffusée uniquement par voie électronique – gratuit – ISSN 1634-0701

Abonnement à partir du site :http://www.alain-bensoussan.com/outils/abonnement-juristendance

Formations intra-entreprise : 2e semestre 2013

LE CABINET A LA QUALITE D'ORGANISME DE FORMATION PROFESSIONNELLE DEPUIS 30 ANS[1].

Archivage électronique public et privé	Dates
▪ Gérer un projet d'archivage électronique : Intégrer les prérequis juridiques dans la conduite du projet et garantir la conformité des systèmes d'archivage électronique.	19-09 et 18-12-2013
▪ Contrôle fiscal des comptabilités informatisées : Prévenir et anticiper les contrôles fiscaux et gérer les contraintes liées à l'évolution des systèmes d'information.	04-07 et 02-10-2013
Cadre juridique et management des contrats	
▪ Cadre juridique des achats : Comprendre les bases du droit de l'achat et gérer les étapes de la conclusion d'un achat, depuis les pourparlers jusqu'au précontentieux.	12-09 et 12-12-2013
▪ Manager des contrats d'intégration et d'externalisation : Comprendre les particularités de l'intégration et de l'outsourcing et bien gérer l'exécution des contrats.	11-07 et 15-10-2013
▪ Contract management : Comprendre les bases du droit des contrats et gérer les étapes de la conclusion d'un contrat, depuis les pourparlers jusqu'au précontentieux.	19-09 et 19-12-2013
▪ Sécurisation juridique des contrats informatiques : Comprendre et mettre en œuvre les outils juridiques de sécurisation des contrats informatiques.	10-07 et 24-10-2013
Conformité	
▪ Risque et conformité au sein de l'entreprise : Cerner le rôle et la place de la conformité dans l'entreprise pour sécuriser l'activité de l'entreprise.	10-07 et 10-10-2013
Informatique	
▪ Edition de progiciel : Etat de l'art et tendances juridiques : Maîtriser le cadre juridique de l'édition logicielle pour gérer l'administration des parcs de progiciels.	04-07 et 07-11-2013
▪ Traitements et hébergement des données de santé à caractère personnel : Identifier les problématiques complexes (contrats d'hébergement, contrats de sous-traitance, etc.) et bénéficier de recommandations spécifiques s'agissant des clauses des contrats.	25-09 et 04-12-2013
Innovation propriété intellectuelle et industrielle	
▪ Audit du patrimoine intellectuel de l'entreprise : Détecter les forces, points de faiblesses et risques juridiques et financiers d'un portefeuille « Propriété Intellectuelle ».	03-07 et 16-10-2013
▪ Protection d'un projet innovant : Présenter les spécificités juridiques relatives à un projet innovant afin de gérer les étapes d'une protection adaptée.	18-09 et 04-12-2013
▪ Sensibilisation à la protection d'un portefeuille marque et nom de domaine : Acquérir la connaissance minimale pour assurer la protection d'une marque et d'un nom de domaine de la création à l'échéance tout en assurant le maintien et la défense.	25-09 et 12-12-2013
▪ Droit des bases de données : Conclure des licences adaptées à ses besoins et connaître et prévenir les risques liés à l'exploitation d'une base de données.	26-09 et 05-12-2013
▪ Droit d'auteur numérique : Acquérir les bons réflexes pour protéger son patrimoine intellectuel et ne pas porter atteinte aux droits d'autrui.	04-09 et 10-12-2013
▪ Lutte contre la contrefaçon : Anticiper les difficultés liées à la contrefaçon sur internet et cerner les spécificités face aux technologies de l'information et de la communication.	26-09 et 06-12-2013

[1] Catalogue de nos formations 2013 sur : http://www.alain-bensoussan.com/secteurs-dactivites/formation-intra-entreprise

Management des litiges

▪ Médiation judiciaire et procédure participative de négociation : Comprendre le déroulement de la procédure de médiation judiciaire et de la procédure participative.	11-07 et 08-10-2013

Internet et commerce électronique

▪ Commerce électronique : Acquérir les connaissances indispensables à la maîtrise des obligations principales d'un éditeur d'un site marchand.	24-09 et 17-12-2013
▪ Webmaster niveau 2 expert : Présentation en 360° des risques juridiques d'une activité web 2.0 et web 3.0.	05-09 et 05-12-2013

Presse et communication numérique

▪ Atteintes à la réputation sur Internet : Gérer les difficultés d'application de la loi sur la presse aux nouveaux vecteurs de communication de la pensée.	02-07 et 03-10-2013

Informatique et libertés

▪ Informatique et libertés (niveau 1) : Identifier et qualifier les intervenants et les responsabilités, prévenir les risques et cerner les formalités obligatoires.	13-09-2013
▪ Cil (niveau 1) : Permettre au Cil de maîtriser les obligations et responsabilités qui lui incombent et de savoir les mettre en œuvre.	27-09-2013
▪ Informatique et libertés secteur bancaire : Sensibiliser les opérationnels sur les risques Informatique et libertés liés aux traitements du secteur bancaire.	22-10-2013
▪ Informatique et libertés collectivités territoriales : Informer les collectivités territoriales sur les modalités d'application de la réglementation Informatique et libertés.	18-10-2013
▪ Sécurité informatique et libertés : Connaître les exigences issues de la réglementation Informatique et libertés en matière de sécurité des données personnelles et sensibiliser aux risques liés à une faille de sécurité.	11-10 et 03-12-2013
▪ Devenir Cil : Mettre en œuvre une politique de protection des données efficace (accountability, etc.) et résoudre les questions complexes (réseaux sociaux, etc.).	05-07 et 04-10-2013
▪ Cil (niveau 2 expert) : Perfectionnement et résolution de questions complexes ; acquisition de méthodologie pour exercer l'activité selon l'approche Privacy by Design.	03-07 et 18-09-2013
▪ Informatique et libertés gestion des ressources humaines : Donner aux membres de la direction des ressources humaines les clés pour utiliser les outils et les traitements de données personnelles mis en œuvre en matière de gestion des ressources humaines.	20-09 et 29-11-2013
▪ Flux transfrontières de données : Présenter les dispositions qui régissent ces flux et élaborer une stratégie de gestion des flux conformément à la loi.	06-09 et 15-11-2013
▪ Contrôles de la Cnil : Connaître l'étendue des pouvoirs de la Cnil et ses moyens de contrôle, apprendre à dialoguer avec la Cnil (notamment par le biais d'un jeu de rôle).	17-09 et 26-11-2013
▪ Informatique et libertés secteur santé : Sensibiliser aux risques Informatique et libertés liés aux traitements du secteur santé et assurances et apporter des éléments de benchmark permettant de positionner son niveau de conformité.	25-10 et 13-12-2013
▪ Formation intra entreprise Informatique et libertés à l'attention du comité exécutif : Sensibiliser les membres du comité exécutif aux risques Informatique et libertés liés à leur activité.	Selon demande

5e édition : Informatique, Télécoms, Internet (actualisée au 10-09-2012)

Informatique, Télécoms, Internet, Editions Francis Lefebvre 5e éd. 2012

▪ Comme pour les quatre premières éditions, l'ouvrage expose toutes les règles juridiques à connaître applicables à l'économie des systèmes d'information et confronte le monde de l'informatique :

- au droit du travail (contrôle des salariés, évaluation professionnelle, etc.) ;

- à la fiscalité (conception et acquisition de logiciels, crédit d'impôt recherche, avantages de l'infogérance, etc.) ;

- aux assurances ;

- au domaine de la santé (carte santé et secret médical, etc.) ;

- à internet et au commerce électronique.

▪ Cette nouvelle édition intègre toutes les nouveautés les plus récentes et notamment :

- les nouveaux contrats d'externalisation (de la virtualisation au cloud computing) ;

- le nouveau CCAG des marchés de l'information et de la communication (TIC) ;

- le nouveau régime de la vidéoprotection issu de la LOPPSI 2 ;

- la E-réputation de l'entreprise (blogs et réseaux sociaux) ;

- la régulation des activités commerciales sur internet ;

- le téléchargement illégal sur internet ;

- l'usurpation d'identité numérique, la régulation des activités commerciales sur internet, etc.

▪ Cette nouvelle édition innove en ajoutant les référentiels normatifs qui font pleinement partie du cadre juridique applicable aux différents systèmes qui traitent l'information : référentiels de système de management de la qualité, de l'environnement et de la sécurité ou d'ingénierie logicielle (CMMI, ISO 20000-1, ITIL, famille ISO 9000, etc.).

▪ Les mises à jour apportées à l'édition 2012 de l'ouvrage Informatique, Télécoms, Internet sont disponibles en ligne.

[2] Nos publications : http://www.alain-bensoussan.com/espace-publication/bibliographie

par Isabelle Pottier

Cyber-risques : l'assurance peut intervenir quand la sécurité n'a pas suffit…

Nicolas Hélénon, Directeur Associé, NeoTech Assurances du groupe LSN Assurances

Pouvez-vous nous dire en quoi consiste votre activité au sein du Groupe LSN ?

NeoTech Assurances est l'entité au sein de LSN Assurances (groupe Diot LSN, 5ème groupe de courtage français) dédiée aux risques du numérique.
Notre activité consiste à accompagner nos clients dans la prévention et dans la gestion de leurs risques et de négocier et de concevoir des contrats d'assurance en adéquation avec leurs risques.
Nous sommes le courtier conseil de Syntec Numérique et nous gérons le programme d'assurance « Syntec Numérique Assurances ».

Quels sont les cyber-risques assurables ? piratage informatique, virus, perte de données, etc. ?

Actuellement, il y a plusieurs offres d'assurance sur le marché provenant essentiellement de compagnies anglo-saxonnes comme Beazley. Il s'agit de couvrir les conséquences (préjudice des tiers, les frais de restauration des données, les pertes financières de l'assuré, les frais de défense, les frais de représentation, les frais de communication et de notification) des atteintes (divulgation, intégrité, disparition) aux données des systèmes d'informations mais aussi à la réputation d'une société.
Avec le futur règlement européen, la notification deviendra une obligation pour toute entreprise, de prévenir ses clients en cas d'atteinte à ses données informatiques. Les contrats du marché couvrent les frais de notification (Data Risks Protection). L'estimation de ce que vaut réellement une donnée n'est pas facile car le contexte local, en particulier la législation a un impact important.
Le coût d'une donnée est estimée à la somme de frais engagés en moyenne pour remédier à un « data breach » (consultants, avocats, agences de communication, etc.). Par exemple en 2011, le coût moyen d'une donnée personnelle pour une entreprise française se situait entre 100 € et 150 €. Parmi les autres faits dommageables qui seront évoqués lors du petit-déjeuner du 19 juin 2013, on peut citer :

- Perte, vol, divulgation non autorisée, altération, destruction de données
- Défaillance du système informatique entrainant une atteinte aux données
- Transmission d'un programme malveillant
- Attaque par déni de service
- Retard ou défaut de révélation des incidents ci-dessus
- Non-respect de la charte de protection des données/loi sur la protection des données, etc.

L'externalisation en mode cloud computing change-t-elle l'analyse du risque ?

Oui, en fonction de la qualité de l'hébergeur. Les activités très porteuses du « cloud computing » exposent les utilisateurs à de nouveaux risques opérationnels tels que la carence de fournisseur, la non disponibilités de données suite à des problèmes réseaux. Donc l'analyse du risque sera impactée par la qualité de l'hébergeur.
Il faut aussi noter que si l'hébergeur subit un data breach (violation de données), le contrat d'assurance du client interviendra en premier lieu et exercera son recours à l'encontre de l'hébergeur et de son assureur RCP. Il peut arriver que la société cliente de l'hébergeur soient assurée additionnel sur la police RC Cyber du prestataire pour permettre à celle-ci d'intervenir en premier lieu et éviter tout recours entre client et prestataire dans les cas où le prestataire serait à l'origine du data breach.