LEXING ALAIN BENSOUSSAN Juristendances Informatique et Télécoms
n° 135 – mai 2013

DEUX NOUVEAUX OUTILS POUR MAITRISER LA SOLUTION CLOUD

La protection des données à caractère personnel

- Le CIGREF (Club Informatique de Grandes Entreprises Françaises), l'IFACI (Institut Français de l'Audit et du Contrôle Internes) et l'AFAI (Association Française de l'Audit et du Conseil Informatiques) ont publié un guide sur le Cloud Computing et la protection des données à caractère personnel (1).
- La démarche des trois associations professionnelles vise à faciliter le dialogue entre les directions métiers et la DSI en expliquant la **réalité des offres Cloud** et leurs limites en matière de protection des données.
- Parmi les **recommandations contractuelles** relatives à la protection des données, notamment l'intégrité et la confidentialité, les trois associations professionnelles rappellent certaines règles.
- Ainsi, dans le cadre d'un service Cloud qui héberge des données à caractère personnel, géré par des **opérateurs offshore** (hors Union européenne), il est nécessaire de s'assurer que l'on est en conformité avec les règlements relatifs aux transferts internationaux de données (déclaration de transferts internationaux, Binding corporate rules ou clauses contractuelles européennes).

Les fondamentaux du Cloud computing

- Parallèlement, le CIGREF a publié un rapport issu de son groupe de travail sur le Cloud computing dans le système d'information de l'entreprise (2).
- Dans ce rapport, il redéfinit les fondamentaux du Cloud computing en fonction de la **compréhension** et de sa mise en œuvre par les entreprises (et non à partir des offres du marché) :

- comment qualifier un cloud ?

- comment ordonner les différents types de cloud ?

- qui gère le cloud ? l'entreprise elle-même ou un opérateur de cloud ?

- qui est le client du service offert par le cloud ? l'entreprise elle-même ou une organisation externe (fournisseur, partenaire, filiale, etc.) ?

- Le CIGREF a identifié quatre typologies de cloud :

- le cloud « **interne** » dans le cas ou c'est l'entreprise qui est maître de la gestion du cloud ;

- le cloud « **externe** » dans le cas ou la gestion du cloud est maîtrisée par un prestataire opérateur de cloud ;

- le cloud « **privé** » s'il est dédié aux besoins propres de l'entreprise ;

- le cloud « **ouvert** » s'il est ouvert au grand public ou à une autre organisation externe à l'entreprise (fournisseur, partenaire, filiale, etc.).

- Le rapport contient un ensemble de **conseils** et de **bonnes pratiques** concernant chacune de ces typologies.

L'essentiel

Pour une meilleure maîtrise de la solution cloud :

- protéger les données à caractère personnel ;

- faciliter le dialogue entre les directions métiers et la DSI ;

- définir de bonnes pratiques juridiques, sécurité et risque, RH et compétences, données et audit, infrastructures.

(1) Guide pratique CIGREF, IFACI et AFAI, mars 2012.

(2) Rapport CIGREF, mars 2012.

JEAN-FRANÇOIS FORGERON
ISABELLE POTTIER

LA GARANTIE CONTRACTUELLE EST ATTACHEE A LA CHOSE ET NON A LA PERSONNE

L'étendue de la garantie contractuelle à l'égard du sous acquéreur

Les enjeux

▪ La garantie contractuelle consentie à l'acheteur d'un bien profite aussi au sous-acquéreur en cas de revente du bien.

▪ En l'espèce, l'**acheteur un véhicule** automobile acquis auprès d'un garage avec une **garantie contractuelle**, pièces et main d'œuvre, de trois mois, l'a ensuite **revendu à un tiers**.

▪ Constatant dès le lendemain un **dysfonctionnement**, ce dernier a demandé au garage de prendre en charge les réparations y afférents au titre de la **garantie contractuelle** (changement de la courroie de transmission).

▪ Devant son refus, le sous-acquéreur du véhicule, l'a assigné en paiement au titre des frais de réparation (1 348 euros) et de la résistance abusive manifestée (500 euros).

▪ La **juridiction de proximité** de Nantes a considéré que l'action du sous-acquéreur était irrecevable du fait de l'**absence de lien contractuel direct** entre celui-ci et le garage mais également en raison du **défaut de qualité pour agir** à son encontre. Il a donc formé un **pourvoi** contre cette décision.

La garantie contractuelle consentie par le vendeur d'un bien est attachée à la chose vendue et non à la personne.

▪ En estimant que « *le sous-acquéreur jouit de tous les droits et actions attachés à la chose qui appartenaient à son auteur de sorte qu'il dispose, le cas échéant, de l'action en responsabilité contractuelle dont l'acheteur aurait bénéficié s'il avait conservé la propriété de ladite chose*», la Cour de cassation a **censuré la décision** et renvoyé les parties devant la juridiction de proximité de Saint-Nazaire.

▪ Elle ajoute qu'en décidant le contraire, la juridiction de proximité **a violé**, par refus d'application, les articles 1134 et 1147 du Code civil et, par fausse application, les articles 1315, alinéa 1er du Code civil et l'article 32 du Code de procédure civile.

(1) Cass 1re civ. n°11-25864 du 6-2-2013.

Le transfert de la garantie contractuelle aux acquéreurs successifs

Les conséquences

▪ Cette décision doit alerter les vendeurs professionnels, lesquels consentent régulièrement ce type de garantie à leurs acheteurs.

▪ En effet, le **vendeur professionnel** doit avoir en tête que la garantie étant accordée à la chose et non à la personne :

- il ne doit pas l'accorder en prenant en compte des considérations personnelles, mais uniquement des **considérations objectives** (solidité de la chose, qualité de la chose, risque raisonnablement encouru, etc.) ;
- il doit garantir le sous-acquéreur qui le lui demande, même en l'absence de production du contrat de vente intervenu entre le l'acquéreur initial et le sous-acquéreur, et ce d'autant plus qu'au regard de la e procédure, la Cour de cassation considère que le sous-acquéreur a effectivement un **droit à agir** au titre de l'article 32 du CPC.

En cas de revente d'un bien par l'acheteur, le sous-acquéreur peut légitimement se prévaloir de ladite garantie auprès du vendeur initial.

▪ Le vendeur professionnel peut toutefois essayer d'**encadrer strictement cette garantie**, notamment en encadrant son champ d'application, lequel devra être le plus restreint possible et, en tout état de cause, **en limitant la durée de la garantie**.

MARIE-ADELAÏDE DE MONTLIVAULT-JACQUOT
ALEXANDRA MASSAUX

LA COUR D'APPEL DE NANCY DONNE UNE NOUVELLE JEUNESSE A LA SIGNATURE ELECTRONIQUE

Le débat sur la preuve de la signature électronique

▪ Il s'agit à l'origine d'une « simple » affaire portée en 2011 devant le Tribunal d'Instance d'Epinal par une banque à l'encontre d'un **particulier** pour dépassement d'une autorisation de découvert et non-paiement.

▪ En l'espèce, entre 2003 et 2008, la banque accorde à son client, un particulier personne physique, successivement, plusieurs crédits sous forme de découvert en compte. En 2008, la dernière autorisation de crédit est « traitée » **par voie électronique**, l'acceptation du client étant formalisée par l'utilisation d'une solution de **signature électronique**.

▪ Après plusieurs mensualités restant impayées, la banque attrait son client en justice. Mais celui-ci ne comparait pas et n'est pas représenté.

▪ Le premier juge se penche sur la réalité de l'**acceptation de l'offre** par le client et par la même, de la réalité de sa signature… électronique. Donnant raison au client, il considère tout simplement qu'il n'avait pas signé le découvert autorisé au motif qu'un simple document imprimé, intitulé « fichier de preuve de la transaction », produit aux débats sans garantie d'authenticité, ni de justification de la sécurisation de la signature employée, était insuffisant pour faire le lien entre l'offre de prêt et ce document

▪ Cette décision n'a pas été sans conséquence et nombre de directions juridiques se sont alertées sur les risques de mettre en œuvre dans l'entreprise une solution basée sur une signature électronique.

Une reconnaissance de principe de la signature électronique

▪ La Cour d'appel de Nancy rappelle la fonction et les **conditions de validité** et **de fiabilité** de la signature électronique :

« *La signature électronique nécessaire à la perfection d'un acte juridique **identifie** celui qui l'appose. Elle manifeste le **consentement** des parties aux obligations qui découlent de cet acte.*

*Lorsqu'elle est électronique, elle consiste dans l'usage d'un **procédé fiable d'identification** garantissant son **lien avec l'acte** auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie conformément aux dispositions du décret n°2001-272 du 30 mars 2001* ».

▪ La Cour d'appel examine alors spécialement l'ensemble des éléments techniques transmis aux débats ayant permis la signature électronique de l'autorisation de découvert, dont « **le fichier de preuve de la transaction** ».

▪ Les juges constatent que ce fichier de preuve est bien émis par une **autorité de certification** (la société Keynectis), que le numéro de l'avenant autorisant le découvert est bien mentionné sur ce fichier de preuve. Ils en déduisent par la même que l'avenant concerné est bien **signé électroniquement par le client**.

▪ La **présomption de fiabilité** de la signature électronique de l'avenant est en l'espèce rapportée par le fichier de preuve technique, consacrant ainsi la signature électronique présumée fiable d'un **document dématérialisé**.

▪ Il s'agit de la première décision significative sur la signature électronique qui se base sur l'examen du « fichier de preuve » d'un acte signé électroniquement.

Les enjeux

Cette décision est d'importance pour tous les prestataires, fournisseurs, et leurs clients, qui souhaitent passer au tout numérique.

Elle a en effet vocation à s'appliquer dans les relations B to B mais aussi B to C.

(1) CA Nancy, RG 12/01383 du 14-2-2013.

Les conseils

L'établissement et la conservation du « fichier de preuve » de la signature électronique de l'acte par l'autorité de certification est essentielle côté prestataire.

Ce fichier de preuve doit également être conforté par le prestataire par une convention de preuve avec ses clients, destinée à sécuriser en amont la signature des documents..

POLYANNA BIGLE

PORTABILITE DES NUMEROS FIXES : LANCEMENT D'UNE CONSULTATION PUBLIQUE

Cadre législatif et réglementaire de la conservation du numéro fixe

▪ A l'instar de ce qui a été réalisé dans le cadre de la portabilité des numéros mobiles, c'est-à-dire de la possibilité pour un abonné de conserver le bénéfice du numéro qui lui a été initialement attribué par un opérateur, le Code des postes et communications électroniques (CPCE) prévoit également qu'un client d'un opérateur de réseau fixe puisse, sous certaines conditions, **conserver son numéro d'appel** lorsqu'il change d'opérateur.

▪ Le cadre juridique de cette **conservation du numéro fixe** a fait l'objet de nombreux travaux, initiés dès 1998, par l'instauration de la procédure dite du « **guichet unique** », dont le but a été de faciliter les démarches de transfert des numéros fixes d'un opérateur à un autre.

▪ Ce cadre a, depuis, été complété et précisé (1), notamment dans le contexte de la transposition en droit interne des directives constitutives du **troisième paquet télécom**, adopté en 2009.

Une évolution des règles rendue nécessaire par l'évolution du contexte

▪ Face au **développement des demandes** de conservation de numéros, y compris celles relatives à des numéros attribués à des opérateurs alternatifs, l'Arcep a décidé de lancer une **consultation publique** sur les procédures qu'elle propose de mettre en place dans ce cadre.

▪ Ces propositions s'inscrivent dans le prolongement d'un certain nombre de constats issus de l'examen des pratiques actuelles du secteur.

▪ En effet, la **portabilité des numéros fixes** a été marquée par un certain nombre de déboires, liés notamment au phénomène des « **écrasements** » à tort de numéros, c'est-à-dire par des demandes de portabilités émises par des opérateurs se prétendant détenteurs d'un **mandat de portabilité** en bonne et due forme émis par un client souhaitant les rejoindre, alors qu'il n'en était rien.

▪ Ce phénomène avait alors conduit l'Arcep à mettre en place, en concertation avec l'ensemble des opérateurs, des **procédures de retour arrière** et d'indemnisation des clients, que l'autorité propose de consolider, notamment au travers d'un **renforcement des contrôles** à réaliser en amont des demandes de portabilité.

▪ De plus, la portabilité peut être affectée par des considérations de nature géographique, de sorte qu'elle ne peut pas toujours être mise en œuvre, par exemple à l'occasion d'un **déménagement** d'une zone géographique de numérotation vers une **zone géographique** dont la numérotation est **différente**.

▪ Par ailleurs, le marché des professionnels est réglementairement encadré différemment que celui du grand public, de sorte que les conditions de mise en œuvre de la portabilité doivent intégrer ces règles spécifiques aux entreprises.

▪ Enfin, le dispositif actuellement pratiqué prévoit la mise en œuvre de la conservation du numéro fixe dans un **délai maximal de 10 jours calendaires**, contre trois jours ouvrés au maximum, en ce compris deux jours ouvrés pour la gestion des échanges d'informations entre opérateurs, au titre des textes adoptés en 2011.

Les enjeux

Améliorer la fluidité du marché de détail en simplifiant le changement d'opérateurs et en améliorant la transparence et l'information des consommateurs.

(1) Art. L.44 CPCE résultant de l'ordonnance n° 2011-1012 du 24 août 2011.

L'essentiel

Un délai de changement d'opérateur en conservant son numéro fixe non géographique réduit de 10 jours calendaires à 3 jours ouvrés.

FRÉDÉRIC FORSTER

LA PRESENTATION DE L'ENTREPRISE NE DOIT PAS INTERFERER DANS LE JUGEMENT DES OFFRES

Le cadre juridique de l'appréciation des candidatures et des offres des candidats à un marché public

- Cet arrêt fait référence aux articles 52 et 53 du Code des marchés publics.
- L'article 52 du Code des marchés publics dispose que « *(...) Les candidatures (...) sont examinées au regard des* ***niveaux de capacités professionnelles****, techniques et financières mentionnées dans l'avis d'appel public à la concurrence, ou, s'il s'agit d'une procédure dispensée de l'envoi d'un tel avis, dans le règlement de la consultation. Les candidatures qui ne satisfont pas à ces niveaux de capacité sont éliminées (...)* ».
- L'article 53 quant à lui prévoit que « *Pour attribuer le marché au candidat qui a présenté l'offre économiquement la plus avantageuse, le pouvoir adjudicateur se fonde : 1° Soit sur une* ***pluralité de critères non discriminatoires*** *et liés à l'objet du marché, notamment la qualité, le prix, la valeur technique (...) et les caractéristiques opérationnelles. D'autres critères peuvent être pris en compte s'ils sont justifiés par l'objet du marché (...)* ».
- Il ressort de ces textes que si le pouvoir adjudicateur est tenu de vérifier les **capacités des candidats** au moment de l'examen des candidatures, il ne lui est pas interdit, s'il est non discriminatoire et lié à l'objet du marché, de retenir un critère ou un **sous-critère** relatif aux **moyens en personnel et en matériel** affectés par le candidat à l'exécution des prestations du marché afin d'en garantir la qualité technique.

Manquements aux obligations de publicité et de mise en concurrence du pouvoir adjudicateur

- Dans le cadre d'un appel d'offres de l'Assistance publique-Hôpitaux de Paris (AP-HP), il était prévu que la valeur technique serait notamment jugée aux vues du **sous-critère** suivant : "**présentation de l'entreprise**".
- Une société non retenue a engagé un **référé précontractuel**, arguant que cet élément ne devrait être analysé qu'au stade de la sélection des candidatures, non dans le jugement des offres.
- Par un arrêt en date du **11 mars 2013**, le Conseil d'Etat a constaté qu'en l'espèce, le sous-critère «présentation de l'entreprise», prévu par l'AP-HP,« *impliquait une simple présentation générale de l'entreprise, sans rapport avec l'exécution technique du marché, qui permettait seulement une appréciation de la capacité professionnelle et technique des candidats et se rapportait à l'examen et à la sélection des candidatures* » (1).
- Il en a conclu que l'AP-HP avait **manqué à ses obligations** de publicité et de **mise en concurrence** et, qu'eu égard à l'importance de ce sous-critère et même si tous les candidats ont obtenu, pour ce sous-critère, la même note, un tel manquement était **susceptible d'avoir lésé la requérante**.

Les enjeux

Le pouvoir adjudicateur ne doit pas confondre les capacités des candidats examinées au stade de la candidature des moyens en personnel et en matériel affectés par le candidat à l'exécution du marché analysés au stade de l'offre.

(1) CE 11-3-2013 n°364706, Assistance publique-Hôpitaux de Paris.

Les conseils

Constitue un manquement à ses obligations de publicité et de mise en concurrence le recours par le pouvoir adjudicateur, au stade de la sélection des offres, à un sous-critère qui se rapportait à la capacité professionnelle et technique des candidats et de leurs employés et donc à l'examen des candidatures.

FRANÇOIS JOUANNEAU
MAGALI GRANIER

UNEPROPOSITION DE DIRECTIVE SUR LA SECURITE DES RESEAUX ET DE L'INFORMATION (SRI)

Assurer un niveau commun élevé de sécurité des réseaux et de l'information

▪ Avec le développement exponentiel des réseaux et des systèmes d'information, la question de leur **sécurité** devient **préoccupante**. La directive proposée en février 2013 vise à assurer un niveau commun élevé de sécurité des réseaux et de l'information (SRI) au sein de l'Union européenne (1).

▪ Dans ce projet, il est demandé aux États membres d'améliorer leur niveau de préparation et leur **coopération mutuelle** et aux acteurs du marché d'adopter les mesures appropriées pour **gérer les risques de sécurité** et signaler les incidents graves aux autorités nationales compétentes.

▪ Les acteurs du marché concernés sont :

- les **prestataires de services** de la société de l'information qui permettent d'autres services de la société de l'information (réseaux sociaux, moteurs de recherche, services informatiques en nuage, etc.) ;

- les **opérateurs d'infrastructures critiques** (fournisseurs d'électricité et de gaz, transporteurs aériens, établissements de crédit, hôpitaux, etc.).

▪ Les administrations publiques et les acteurs du marché doivent :

- **prendre les mesures techniques** et organisationnelles nécessaires pour gérer les risques qui menacent la sécurité des réseaux et systèmes informatiques qu'ils contrôlent et utilisent dans le cadre de leurs activités (systèmes et réseaux privés qui sont gérés par leur propre service informatique ou dont la gestion de la sécurité a été sous-traitée) ;

- **notifier à l'autorité compétente** les incidents qui ont un impact significatif sur la sécurité des services essentiels qu'ils fournissent.

Mettre en place un système d'alerte rapide et de notification SRI

▪ En **janvier 2012**, seules 26% des entreprises de l'Union européenne avaient une politique de sécurité informatique en bonne et due forme (source Eurostat).

▪ C'est pourquoi, la proposition de directive donne pour **mission à l'autorité compétente**:

- d'informer le public lorsqu'elle jugera qu'il est de l'intérêt général de divulguer les informations relatives à l'incident ;

- de donner des instructions contraignantes aux acteurs du marché et aux administrations publiques ;

- d'exiger des acteurs du marché et des administrations publiques qu'ils fournissent les documents relatifs à leur politique de sécurité et se soumettent à des audits ;

- de coopérer avec l'autorité chargée de la protection des données en cas d'incident portant atteinte à des données à caractère personnel ;

- de notifier aux services répressifs les incidents pouvant constituer une infraction pénale grave.

▪ En France, l'autorité compétente serait l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui est depuis 2009, l'autorité nationale en matière de sécurité et de défense des systèmes d'information.

▪ Elle a notamment pour mission d'assurer la **sécurité des systèmes d'information de l'État** et de veiller à celle des opérateurs nationaux d'importance vitale.

Les enjeux

Accroître la sécurité de l'internet et des réseaux et systèmes informatiques privés et publics sur lesquels reposent les services dont dépend actuellement le fonctionnement de la société et de l'économie.

(1) Proposition de directive, Doc Sénat COM (2013) 48 final du 7-2-2013.

Les conseils

- Contrôler la sécurité et l'encombrement du réseau informatique, mettre en place des mesures techniques de sécurité.

- Rédiger des chartes informatiques qui formalisent notamment les règles d'utilisation du matériel informatique, de l'utilisation d'appareils personnels sur le lieu de travail (BYOD), des connections internet et de la messagerie professionnelle.

VIRGINIE BENSOUSSAN-BRULE

ADVERGAME OU LE MARKETING PAR LE JEU

L'année 2013 : l'année des « advergames »

L'enjeu

Conquérir de nouveaux profils, fidéliser et transmettre des messages.

Eviter que l'advergame ne soit censuré.

▪ Ce **néologisme** composé de la contraction des termes « advertisement » et « game » désigne un **outil marketing** de communication et de promotion dont les performances en termes de dialogue, d'immersion du consommateur dans l'univers de la marque sont très appréciées, en raison essentiellement de la mécanique de jeu qui le caractérise.

▪ Fonctionnant sur l'**interactivité**, un « advergame » permet non seulement de mieux connaître les consommateurs en **collectant des données** les concernant, de les fidéliser mais également de recruter de nouveaux profils en y intégrant, par exemple, des **opérations de parrainage** tout en délivrant des messages de la marque.

▪ L'advergame (ou "jeu vidéo publicitaire") est donc très encadré.

Les advergames : publicité ludique

Les conseils

Respecter les règles déontologiques en matière de publicité

Aller dans le sens de la responsabilité sociale

Etre transparent, loyal et identifiable

Collecter des données dans le respect de la loi informatique et libertés.

▪ L'advergame emprunte les **caractéristiques d'une publicité** qui permet à l'annonceur, de présenter visuellement ou oralement, de manière ludique, ses produits, ses services, son nom, sa marque ou ses activités.

▪ Par conséquent, comme pour toute publicité, l'annonceur devra veiller notamment, sous peine de voir son advergame censuré, à :

- ne pas présenter ses produits, services ou marques de manière contraire aux exigences de la **diligence professionnelle** ;
- éviter d'avoir recours à des moyens, procédés susceptibles d'altérer de manière substantielle, le comportement économique du consommateur normalement informé et raisonnablement attentif et avisé ;
- respecter les **règles déontologiques** applicables à la publicité en particulier celles définies par l'ARPP (Autorité de régulation professionnelle de la publicité) (1) ;
- que son advergame ne constitue pas une **loterie prohibée**, s'il s'inspire de ce mécanisme.

▪ A cet égard, les annonceurs peuvent utilement se reporter à la **recommandation de l'ARPP du 20 décembre 2010** qui couvre toute forme de communication publicitaire, qu'elle soit, par exemple, diffusée sur les supports mobiles, dans le cadre des Services de Médias Audiovisuels à la Demande, des réseaux sociaux, les « Advergames », la publicité virale, etc.

▪ En complément de sa recommandation, l'ARPP a publié une grille d'interprétation d'une quinzaine de pages conçues pour être lues en complément du texte principal (2).

▪ Enfin, rappelons que lorsque l'advergame permet la **collecte de données**, celle-ci devra s'effectuer dans le respect de la **loi informatique et libertés**.

▪ A ce titre, s'agissant plus particulièrement de l'**attrait des mineurs** pour ce type de publicité très ludique, l'ARPP les encourage, notamment sur les formulaires de saisie, à demander la **permission des parents** ou de leurs responsables légaux avant de fournir des informations personnelles.

▪ Elle recommande aux annonceurs de **ne pas collecter** par le biais d'un enfant les données à caractère personnel d'un tiers.

(1) Recommandation déontologique ARPP « Internet V 3.0 ». du 20-12-2010.
(2) Grille d'interprétation de la recommandation du 20-12-2010.

CELINE AVIGNON

LES ROBOTS ET LE DROIT DES MARQUES : L'EMERGEANCE DES MARQUES ROBOTIQUES

La personnalité juridique du robot et le droit des marques

L'enjeu

▪ Un **statut juridique spécifique** pourrait être reconnu aux robots, en particulier aux robots de services, à l'issue des réflexions qui agitent le monde de la robotique.

▪ Ce **secteur innovant et émergent** a été présenté pour la troisième année consécutive dans le cadre de l'événement international INNOROBO qui s'est tenu à Lyon du 19 au 21 mars 2013 et qui fait l'objet d'un plan robotique.

▪ Ces discussions ont une répercussion directe sur la stratégie de **protection des noms des robots** par le droit des marques (1).

La protection du robot par le droit des marques

▪ Deux hypothèses s'offrent aux créateurs de robots :

- soit le robot reste à l'état de **produit**, comme il l'est pour les robots industriels actuels ;

- soit, à l'inverse, confronté à des robots de plus en plus intelligents et autonomes, le législateur vient à leur reconnaître une **personnalité juridique ad hoc** comparable à celle reconnue aux entités dotées d'une existence juridique (sociétés commerciales, associations, etc.), leur conférant des **droits** et des **obligations**.

L'influence de la personnalité juridique du robot sur les marques robotiques.

▪ La **stratégie de protection** du nom du robot n'est pas la même dans les deux hypothèses.

(1) Cf. notre article paru dans L'Usine nouvelle, le 4 avril 2013.

La stratégie de protection d'une marque robotique

Les conseils

▪ Dans le **premier cas**, la protection efficace du nom du robot continuera à être réalisée, comme elle l'est actuellement, par un **enregistrement de marque** revendiquant les **produits " robot "**, désignation expressément prévue à deux reprises dans la classification internationale des marques de Nice dans la **classe 7** pour " le robot (machine) " et les " robots de cuisine électriques ".

▪ Cette répartition n'exclue pas une **probable modification** de la classification de Nice dans le cadre du Comité d'Experts de l'Union de Nice pour tenir compte de l'**évolution des technologies** et des domaines concernés.

Rédiger avec précision le libellé des produits et services dont la protection est revendiquée par l'opérateur économique.

▪ Dans le **second cas**, la stratégie de protection du nom du robot par le droit des marques en serait bouleversée.

▪ La protection accordée aux robots par le droit des marques devrait alors se **détacher des classes de produits** pour s'orienter vers les **classes de services** afin de désigner les services que le robot sera susceptible de rendre, comme par exemple les services de nettoyage, de bâtiments, de jardinage, de transport, de livraison de marchandises, d'éducation, de chirurgie, aide à la personne, etc.

▪ Face à ces interrogations et compte tenu de la longévité d'une marque qui reste indéfiniment renouvelable, il est recommandé d'être attentif présentement à la rédaction des libellés revendiqués pour les marques robotiques et de ne pas limiter le libellé aux produits " robots " et aux produits complémentaires.

▪ Il convient en effet d'**anticiper** sur une possible personnalité juridique, en **étendant le champ du libellé** aux services que le robot sera susceptible de rendre sous la marque enregistrée.

CLAUDINE SALOMON
ANNE-SOPHIE CANTREAU

L'ADMINISTRATION FICALE PEUT SAISIR DES DONNEES SUR DES SERVEURS A DISTANCE

Le contribuable ne peut plus s'opposer aux saisies de données informatiques

▪ En application de l'article L.16 B du Livre des procédures fiscales (LPF), l'administration fiscale peut être autorisée par le **juge des libertés** et de la détention, à effectuer des **visites** en tous lieux, mêmes **privés**, où des pièces et **documents révélant une fraude à l'impôt** sur le revenu ou sur les bénéfices ou à la TVA sont susceptibles d'être détenus et procéder à leur saisie, quel qu'en soit le support.

▪ Avant le vote de ces nouvelles dispositions, le contribuable pouvait refuser de donner accès aux données informatiques notamment sur des serveurs situés à distance sans être sanctionné.

▪ Désormais, dans l'hypothèse où le contribuable fait obstacle à l'accès aux pièces ou documents présents sur un **support informatique**, à leur lecture ou à leur saisie, l'administration mentionne ce refus sur le procès-verbal. Les agents de l'administration fiscale peuvent alors procéder à la **copie de ce support** et le placer **sous scellés**.

▪ Ils disposent, alors, d'un délai de **quinze jours** à compter de la date de la visite pour accéder aux documents qui y sont contenus, les lire et les saisir, et restituer le support. Ce délai de quinze jours peut être **prorogé** par le juge.

La procédure de saisie de données informatiques

▪ Ces dispositions ne doivent servir qu'aux opérations nécessaires à l'accès ou à la mise au clair des données contenues sur la copie du support.

▪ Le contribuable ou son représentant est avisé qu'il peut assister à l'**ouverture des scellés**, à la lecture et à la saisie des pièces et documents du support, qui ont lieu **en présence de l'officier de police** judiciaire.

▪ Un **procès-verbal décrivant les opérations** réalisées est dressé par les agents de l'administration et un **inventaire des pièces** et documents saisis est annexé. Ils sont signés par les agents de l'administration, l'officier de police judiciaire et le contribuable ou son représentant. En son absence ou en cas de refus de signer, une mention en est faite au procès-verbal.

▪ L'administration procède en même temps à la **restitution du support** et de sa copie en main propre ou accomplie sans délai, toutes diligences pour les restituer en cas d'absence du contribuable.

▪ L'administration fiscale ne peut opposer au contribuable les informations recueillies qu'après restitution des pièces et documents saisis ou de leur reproduction et mise en œuvre des procédures de contrôle fiscal (3).

▪ Rappelons que les **bases d'imposition sont évaluées d'office** lorsque le contrôle fiscal ne peut avoir lieu du fait du contribuable ou d'un tiers.

▪ L'**évaluation d'office pour opposition** à contrôle fiscal peut aussi être mise en œuvre dans le cadre de contrôle faisant suite à une perquisition fiscale au cours de laquelle le contribuable refuse de communiquer des documents tenus sur support électronique.

L'enjeu

La loi de finances rectificative pour 2012 autorise, désormais, l'administration fiscale à saisir des données informatiques se trouvant sur des serveurs situés à distance dès lors qu'elle peut accéder à ces dernières depuis un ordinateur se trouvant dans tous lieux du contribuable vérifié (2).

(1) LPF, art. L.16 B-IV bis nouveau.
(2) Loi de finances rectif. 2012, art. 11-I-2e.

Les conseils

Les nouvelles sanctions fiscales applicables au refus opposé aux agents des impôts d'accéder aux pièces ou documents tenus sur support informatique, à leur lecture ou à leur saisie exigent une vigilance particulière.

(3) LPF, art. L.16 B – VI modifié.

PIERRE-YVES FAGOT

ACTUALITE

Mode d'évaluation des salariés dit du « ranking par quotas »

Les conseils

▪ Si la pratique du **ranking par quotas** n'est pas prohibée par principe, l'évaluation des salariés doit être fonction de leurs **performances** et de leurs **compétences individuelles**.

▪ La mise en œuvre de cette méthode d'évaluation des salariés peut présenter un caractère illicite.

▪ Ainsi dans un arrêt du **27 mars 2013**, la chambre sociale de la Cour de cassation vient de rappeler que la mise en œuvre d'un mode d'évaluation reposant sur la création de **groupes affectés de quotas préétablis** que les évaluateurs sont tenus de respecter est illicite.

Pour être licite, un système d'évaluation doit être fondé sur des critères « objectifs et transparents ».

▪ En l'espèce, bien qu'il existe au sein de la société un système d'évaluation fondé sur des **quotas**, ces derniers sont **indicatifs** et **non impératifs**. La Cour de cassation a donc rejeté le pourvoi du comité d'entreprise de la société et des syndicats.

▪ Elle a considéré que « *si la mise en œuvre d'un mode d'évaluation reposant sur la création de groupes affectés de quotas préétablis que les évaluateurs sont tenus de respecter est illicite, la cour d'appel, appréciant souverainement les éléments de preuve qui lui étaient soumis, a retenu qu'il n'était pas fait application au sein de la société HPF du « ranking » par quotas* ».

(1) Cass. soc. 27-3-2013, n° 11-26539.

Système de vote électronique et confidentialité des données transmises

Les conseils

▪ Le système de vote électronique retenu pour les **élections professionnelles** doit assurer la **sécurité** et la **confidentialité** des données transmises, notamment :

- des fichiers constitués pour établir les listes électorales des collèges électoraux ;

- de l'adressage des moyens d'authentification, d'émargement, d'enregistrement et de dépouillement des votes.

La Commission nationale informatique et libertés (Cnil) préconise la transparence par le recours systématique à l'expertise indépendante et l'accès au code source des logiciels.

▪ Cette confidentialité n'est pas assurée lorsque les **codes personnels** d'authentification sont **adressés** aux salariés sur la **messagerie professionnelle**, **sans autre précaution** destinée notamment à éviter qu'une personne non autorisée puisse se substituer frauduleusement à l'électeur.

▪ En l'espèce, chaque électeur a reçu du prestataire Election Europe, un code PIN secret et un mot de passe, à son domicile par **courrier simple** et sur sa **boîte mail professionnelle non sécurisée**.

▪ La Cour de cassation a considéré que la conformité des modalités d'organisation du scrutin aux **principes généraux du droit électoral** n'était pas assurée, en particulier au regard des articles R. 2314-9 et R. 2324-5 du Code du travail et de l'article L 57-1 du Code électoral.

(2) Cass. soc. 27-02-2013, n° 12-14415.

EMMANUEL WALLE
ISABELLE POTTIER

▪ Elle a donc **cassé** et **annulé** le jugement rendu le 7 février 2012 par le Tribunal d'instance de Versailles et renvoyé l'affaire devant le Tribunal d'instance de Poissy.

Déployer le télétravail : les clés d'une stratégie juridique gagnante : 15 mai 2013

▪ **Emmanuel Walle**, directeur du département « Droit du travail numérique » animera un petit-déjeuner débat consacré aux modalités de déploiement du télétravail. Son déploiement dans une société, une administration ou une association doit répondre aux innovations introduites par la législation. La loi « Warsmann » du 22 mars 2012 a inséré dans la Code du travail, la modulation du temps de travail.

▪ Pourtant la pratique a été largement anticipée, faisant de manière empirique la distinction entre les régimes du télétravail, travail à domicile et nomadisme.

▪ Si le taux de satisfaction liée à cette disposition avoisine les 96 % toutes parties prenantes confondues (employeurs, salariés managers), 92 % d'entre elles considèrent que le premier frein à son développement est la réticence des managers intermédiaires.

▪ Nous vous proposons à l'occasion de ce petit-déjeuner d'examiner les questions qui se posent avant la mise en œuvre d'un projet d'introduction du télétravail :

•Pourquoi mettre en place le télétravail ?

•Comment le mettre en œuvre concrètement ?

•Quel suivi assurer ?

•Quel partage des coûts et responsabilité ?

•Quel est le bilan contentieux du télétravail aujourd'hui ?

▪ Xavier de Mazenod, spécialiste de la communication d'influence, des réseaux sociaux et du télétravail et co-organisateur du Livre blanc du Tour de France du télétravail 2012 sera présent.

▪ **Inscription gratuite** sous réserve de nous confirmer votre présence avant le 13 mai 2013 en renseignant le formulaire en ligne.

Impact du bilan d'activité de la Cnil sur les entreprises : 31 mai 2013

▪ **Alain Bensoussan** animera un petit-déjeuner débat consacré au 33e rapport de la Cnil et aux plans de mise en conformité qui s'imposent aux entreprises pour anticiper la réforme du cadre légal européen en matière de protection des données.

▪ L'année 2012 a été marquée par une forte activité pour la Cnil. Elle a en effet reçu un nombre record de plaintes (6017 : soit + 4,9 % par rapport à 2011) dont on peut relever la répartition suivante :

•31 % dans le secteur de l'internet et des télécoms en grande partie sur le « droit à l'oubli numérique » (1 050 plaintes ont concernées la suppression de textes, photographies, vidéos, coordonnées ou commentaires)

•15 % dans le secteur du travail (vidéosurveillance, géolocalisation, accès au fichier professionnel)

•10 % dans le secteur bancaire (inscription au FICP, FCC, etc.)

▪ Elle a réalisé 458 contrôles (soit +19% par rapport à 2011) qui ont abouti à 43 mises en demeure, 4 sanctions pécuniaires, 9 avertissements, 1 injonction de cesser le traitement. Les contrôles ont surtout portés sur :

• les dispositifs de vidéoprotection : 173 contrôles

• les données personnelles et la vie quotidienne : des contrôles de grande ampleur ont été réalisés notamment auprès des fournisseurs d'énergie, de services de communications électroniques et de sociétés d'autoroute

• la sécurité des données de santé : une vingtaine de contrôles ont été effectués auprès d'hébergeurs agréés, pharmaciens, groupe hospitalier, laboratoires d'analyse médicale, prestataires développant des logiciels ou produits destinés à traiter des données de santé

• les failles de sécurité : de nombreux contrôles ont été réalisés dans le cadre d'alertes reçues par la Cnil

▪ L'activité s'annonce aussi riche en actions pour 2013-2014, au vu du programme des contrôles annoncés.

▪ Nous vous proposons à l'occasion de ce petit-déjeuner d'aborder les d'actions qui s'imposent aux entreprises au vu du bilan d'activité de la Cnil et du projet de Règlement européen sur la protection des données personnelles qui sera très prochainement adopté.

▪ **Inscription gratuite** sous réserve de nous confirmer votre présence avant le 29 mai 2013 en renseignant le formulaire en ligne.

NOTRE RESEAU DE CORRESPONDANTS ORGANIQUES LEXING VOUS INFORME

La Cour européenne rejette le recours de « Pirate Bay »

Lexing Luxembourg

▪ Suite à la plainte de plusieurs titulaires de droits de propriété intellectuelle contre le site de téléchargement « The Pirate Bay », ses cofondateurs ont été condamnés pour **complicité de violation de la loi suédoise** sur le droit d'auteur, le 17 avril 2009 par le Tribunal de District de Stockholm, à une peine d'un an de prison ainsi qu'à des dommages et intérêts à hauteur de 3,3 millions d'euros.

▪ Le 26 novembre 2010, la Cour d'appel (Sveahovrätt) a confirmé, dans les grandes lignes, le jugement. Le 1er février 2012, la Cour Suprême de Suède a refusé le recours introduit par les fondateurs du site web.

Cabinet Philippe &Partners

▪ Ces derniers ont alors introduit, le 20 juin 2012,un recours **devant la Cour Européenne des Droits de l'Homme** en arguant qu'ils n'avaient eux-mêmes commis aucune atteinte à la propriété intellectuelle de tiers, mais simplement mis en place un système permettant d'échanger des informations. L'éventuel usage illicite de ces services par l'utilisateur final relèverait alors de la responsabilité de ce dernier et non des créateurs du service. La condamnation pour complicité d'atteinte au droit d'auteur violerait donc le droit à la liberté d'expression garanti par l'article 10 de la Convention.

Actualité du 25-3-2013.

▪ L'argument, bien que séduisant, n'a pas été accueilli par la Cour, qui a déclaré le **recours irrecevable** par une décision du 19 février 2013.

Nouvelle jurisprudence vaudoise en matière de vidéosurveillance en milieu scolaire

Lexing Suisse

▪ Dans un arrêt du 1er mars 2013, la cour de droit administratif et public du tribunal cantonal a considéré que l'installation d'un système de vidéosurveillance par la Commune de Lutry pour surveiller les espaces extérieurs de deux établissements scolaires, y compris pendant les heures de cours, respecte le **principe de proportionnalité** au sens étroit dès lors que les élèves et les enseignants ne sont filmés qu'à l'extérieur des bâtiments scolaires. L'impact sur l'enseignement lui-même et la personnalité des élèves doit par conséquent être relativisé.

Cabinet Sébastien Fanti.

Réforme code de commerce Marocain : moins de formalisme

Lexing Maroc

▪ Les modifications apportées par le projet de loi 08-11 réformant le code de commerce Marocain propose notamment que l'immatriculation au registre de commerce soit précédée de l'identification à l'administration fiscale par l'**attribution de l'identifiant fiscal unique (IFU)**.

▪ Ainsi, ce numéro sera généré dès la première étape du processus de création d'une entreprise commerciale, personne physique ou morale et le greffier auprès duquel s'effectue l'immatriculation exigera l'IFU plutôt que la taxe professionnelle.

Cabinet Bassamat& Associée, Fassi-FihriBassamat

▪ D'autant plus que l'imposition à cette taxe est davantage liée au début d'activité de l'entreprise qu'à la phase préalable de sa création. L'IFU n'intervient pas seulement au moment de la constitution de l'intervention.

Actualité du 08-4-2013.

▪ Il sera désormais exigé lors de la remise d'un chèque (art. 251), de l'ouverture d'un compte bancaire (art. 488).

Publication du rapport d'activité de la Cnil 2012

▪ La Cnil vient de publier son **33ème rapport d'activité 2012** (1). L'année a été marquée par une forte augmentation des activités de contrôle et de sanction de la Cnil. Ainsi, 458 contrôles ont été effectués en 2012 soit une croissance de 19 % par rapport à l'année 2011.

(1) Cnil 33ème rapport d'activité 2012.

Ratification du traité de Beijing par la République arabe syrienne

▪ La République Arabe Syrienne est le **premier Etat à avoir ratifié** (2) le Traité de Beijing sur la protection des artistes dans le domaine de l'audiovisuel signé le 26 juin 2012 par les négociateurs des Etats membres de l'OMPI.

(2) Notification Beijing n°1 du 18-3-2013.

Cloud Computing et protection des données

▪ Le **CIGREF** (Club Informatique de Grandes Entreprises Françaises), l'**IFACI** (Institut Français de l'Audit et du Contrôle Internes) et l'**AFAI** (Association Française de l'Audit et du Conseil Informatiques) ont publié un guide sur le Cloud Computing et la **protection des données à caractère personnel** pour faciliter le dialogue entre les directions métiers et la DSI(3).

(3) Guide pratique CIGREF, IFACI et AFAI, Mars 2013.

▪ Parallèlement, le CIGREF a publié un rapport issu de son groupe de travail sur le Cloud computing dans le SI de l'entreprise, dans lequel il redéfinit les **fondamentaux du Cloud** computing (4).

(4)Rapport CIGREF, Mars 2013.

Recommandations du G29 sur les applications mobiles pour smartphones

▪ Dans un avis a publié le **14 mars 2013**, le groupe des Cnil européennes (G29) a précisé les règles applicables aux smartphones en matière de **protection des données à caractère personnel** (5).

(5) G29 WP 202 Opinion 02-2013 on apps on smart devices EN, publié le 14-3-2013.

La Cnil et 5 autres autorités européennes lancent une action contre Google

▪ Six autorités européennes de protection des données ont chacune lancé des actions contre Google.

▪ La Cnil a, pour sa part, notifié à Google sa **décision d'ouvrir une procédure** de contrôle ainsi qu'une procédure de coopération internationale avec ses homologues européens. Google va se faire assisté, dans ce cadre, de spécialistes du domaine Informatique et libertés (6).

(6) Actualité Cnil du 2-4-2013.

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 : 1er semestre 2013

Le cabinet a la qualité 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.	31-01 et 25-04-2013
▪ **Contrôle fiscal des comptabilités informatisées** : Prévenir et anticiper les contrôles fiscaux et gérer les contraintes liées à l'évolution des systèmes d'information.	09-01 et 03-04-2013
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.	12-02 et 06-06-2013
▪ **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.	05-02 et 16-05-2013
▪ **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.	21-02 et 30-05-2013
▪ **Sécurisation juridique des contrats informatiques**: Comprendre et mettre en œuvre les outils juridiques de sécurisation des contrats informatiques.	17-01 et 17-04-2013
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.	23-01 et 18-04-2013
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.	28-02 et 23-05-2013
▪ **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.	13-06-2013
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 ».	14-02 et 26-04-2013
▪ **Protection d'un projet innovant**: Présenter les spécificités juridiques relatives à un projet innovant afin de gérer les étapes d'une protection adaptée.	19-03 et 12-06-2013
▪ **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.	27-02 et 17-04-2013
▪ **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.	7-04 et 22-05-2013
▪ **Droit d'auteur numérique**: Acquérir les bons réflexes pour protéger son patrimoine intellectuel et ne pas porter atteinte aux droits d'autrui.	06-02 et 15-05-2013
▪ **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.	28-03 et 20-06-2013

[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.	15-01 et 09-04-2013
Internet et commerce électronique	
▪ **Commerce électronique**: Acquérir les connaissances indispensables à la maîtrise des obligations principales d'un éditeur d'un site marchand.	24-01 et 16-04-2013
▪ **Webmaster niveau 2 expert**: Présentation en 360° des risques juridiques d'une activité web 2.0 et web 3.0.	17-01 et 04-04-2013
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.	8-01 et 02-04-2013
Informatique et libertés	
▪ **Informatique et libertés (niveau 1)**: Identifier et qualifier les intervenants et les responsabilités, prévenir les risques et cerner les formalités obligatoires.	11-01 ; 29-03 et 07-06-2013
▪ **Cil (niveau 1)**: Permettre au Cil de maîtriser les obligations et responsabilités qui lui incombent et de savoir les mettre en œuvre.	18-01 ; 15-03 et 21-06-2013
▪ **Informatique et libertés secteur bancaire**: Sensibiliser les opérationnels sur les risques Informatique et libertés liés aux traitements du secteur bancaire.	22-01 ; 28-03 et 11-06-2013
▪ **Informatique et libertés collectivités territoriales**: Informer les collectivités territoriales sur les modalités d'application de la réglementation Informatique et libertés.	25-01 ; 8-03 et 14-06-2013
▪ **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.	22-02 et 28-06-2013
▪ **Devenir Cil**: Mettre en œuvre une politique de protection des données efficace (accountability, etc.) et résoudre les questions complexes (réseaux sociaux, etc.).	08-02 et 05-04-2013
▪ **Cil (niveau 2 expert)**: Perfectionnement et résolution de questions complexes ; acquisition de méthodologie pour exercer l'activité selon l'approche Privacy by Design.	13-02 et 24-04-2013
▪ **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.	15-02 et 12-04-2013
▪ **Flux transfrontières de données**: Présenter les dispositions qui régissent ces flux et élaborer une stratégie de gestion des flux conformément à la loi.	22-02 et 19-04-2013
▪ **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).	26-02 et 23-04-2013
▪ **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.	01-03-2013
▪ **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