



LA DEMATERIALISATION DES PROCEDURES CONTENTIEUSES ADMINISTRATIVES

L'application web « télérecours »

- Le décret en date du 21 décembre 2012 (1) met en place une application web « télérecours ».
- Ce service permet de **transmettre, par voie électronique**, toutes les productions (requêtes, mémoires et pièces) et de recevoir de la juridiction tous les **actes de procédure** (communication, mesures d'instruction, avis d'audience, notification des décisions pour les administrations et transmission de leurs ampliations pour les avocats).
- Ce service est ouvert, à tous les stades de la procédure contentieuse, aux **avocats** et aux **administrations** (ainsi qu'aux organismes de droit privé assimilés tels que les caisses primaires d'assurance maladie) pour **l'ensemble des contentieux**, quel que soit leur objet et la nature de la procédure.
- Cette application est expérimentée, depuis plusieurs années déjà, au Conseil d'Etat et dans les juridictions franciliennes pour le contentieux d'assiette en matière fiscale. Le décret généralise et **pérennise l'expérimentation**.
- L'application va être **progressivement généralisée** au cours de l'année 2013. Elle sera, dans un premier temps, déployer **dès le 2 avril 2013** auprès du Conseil d'Etat, des cours administratives d'appel de Nancy et de Nantes et des tribunaux administratifs de leur ressort, **puis à l'automne 2013** auprès des six autres cours administratives d'appel et leurs tribunaux.

Développement de la signature électronique

- Cette plateforme permettra aux parties de **signer leur production par voie électronique**, conformément aux prescriptions de l'article 1316-4 du Code civil, si elles disposent d'un **certificat électronique**, à cet effet.
- Pour bénéficier de l'application Télérecours, les parties devront préalablement s'y inscrire. Elles figureront alors dans un **annuaire national** valable devant toutes les juridictions administratives. Elles pourront être ainsi **authentifiées** à chacune de leurs utilisations de l'application.
- Les avocats pourront utiliser le **certificat** dont ils disposent dans le cadre du RPVA ou de la procédure dématérialisée avec la Cour de cassation.
- Pour les dossiers dont les mémoires et les pièces auront fait l'objet de communications écrites traditionnelles, elle offrira les mêmes informations sur la procédure et l'état du dossier que celles aujourd'hui accessibles par l'application SAGACE.
- Cette **signature ne sera pas obligatoire**. En l'absence de signature électronique, les parties seront simplement astreintes à conserver par devers elle un exemplaire écrit de leur production revêtu d'une signature manuscrite, de manière à être en mesure de le produire en cas de nécessité.

L'enjeu

Le site constitue un outil de gestion de sécurisation des échanges entre les parties et les tribunaux offrant une accessibilité immédiate au contenu de l'ensemble des dossiers dont les mémoires et les pièces auront été ainsi communiqués.

(1) [Décr. n°2012-1437 du 21-12-2012.](#)

Les conseils

En l'absence de certificat électronique, les parties devront conserver un exemplaire écrit de leur dossier.

[FRANÇOIS JOUANNEAU](#)

[MAGALI GRANIER](#)



LE PLAN DE SOUTIEN AU SECTEUR DE LA ROBOTIQUE : ENJEUX ETHIQUES ET JURIDIQUES

Le gouvernement prépare un plan de soutien de la robotique

- En octobre 2012, le ministre du redressement productif annonçait la préparation d'un **plan de soutien au secteur de la robotique** (1). Ce plan qui doit être dévoilé dans les prochaines semaines, devrait comporter des mesures incitant les petites entreprises à se lancer dans la robotisation (2).
- De son côté, le nouveau **Conseil national de l'industrie** (CNI), qui remplace la conférence nationale de l'industrie créé il y a deux ans par Nicolas Sarkozy, a pour mission d'élaborer des **contrats de filières** dans chacune des douze identifiées dont la filière robotique.
- Un nouveau comité de filières doit se réunir le **19 mars 2013** sur la robotique. Selon Bercy, des **fonds sectoriels** pourraient être débloqués pour les secteurs de la robotique et de la sécurité (3).
- Cette mobilisation fait écho à l'étude parue en **juin 2012**, sur l'avenir de la filière robotique en France, et plus particulièrement de la **robotique de service**, c'est-à-dire celle « *qui assiste l'homme dans ses activités professionnelles comme dans sa vie courante, contribuant à améliorer ses conditions de travail, sa sécurité, son bien-être* » (robots ménagers, aspirateurs, jouets humanoïdes, assistants médicaux, etc.) (4).
- Après une première partie sur l'état des lieux de la filière, l'étude s'intéresse prioritairement à trois marchés émergents pour la robotique de service : l'**assistance** à la personne en perte d'autonomie, les robots **compagnons** ou robots domestiques et les robots de **surveillance** et de gardiennage.
- Le marché global de la robotique de service est aujourd'hui porteur d'un **potentiel très important** en France et dans le monde, et l'on estime que les marchés de robotique de service personnelle comme professionnelle devraient doubler entre 2010 et 2015.

Les enjeux éthique et juridique

- L'étude s'est penchée sur la question du droit. La réglementation peut en effet, être un **accélérateur** ou un **frein** pour le développement de la robotique de service.
- En France comme en Europe, les cadres réglementaire et éthique sont encore assez flous. Or, l'acceptabilité juridique pose deux questions :
 - La question de la **responsabilité**, majeure pour les industriels : Elle amène à s'interroger « sur les transferts de responsabilité possibles de l'utilisateur vers le fabricant du robot », à mesure que le degré d'autonomie dont dispose le robot s'accroît. Qui sera responsable lorsqu'il prendra une décision portant préjudice à une personne, notamment en cas de dysfonctionnement ?
 - La question de la **légalité** éventuelle de certains dispositifs : certains types de robots, en environnement professionnel comme domestique, peuvent poser des questions relatives aux **libertés individuelles** (respect de la dignité de la personne humaine, de la vie privée, des libertés individuelles, de la confidentialité et du secret médical, etc.).
- Les robots domestiques de surveillance sont de véritables **espions** qui collectent et manipulent des **données personnelles**. L'enjeu en matière de vie privée sera donc majeur dans les années à venir.
- Il s'agit là de vraies questions, pour un domaine appelé à devenir la **prochaine révolution technologique** ou « rovolution » (5), après l'invention de l'informatique au 20 e siècle.

L'enjeu

La robotique est considérée comme un élément clé de la compétitivité des entreprises industrielles, au point de susciter des soutiens publics.

(1) En ouverture des [Assises de l'industrie](#) organisées par l'Usine Nouvelle, le 17-10-2012.

(2) [Les Echos.fr du 5-3-2013](#).

(3) [L'Usine Nouvelle du 5-2-2013](#).

(4) [Etude DGCISPIPAME 2012](#).

(5) Bruno Bonnell, « Viva la rovolution ! », Ed. JC Lattès, mai 2010.

L'essentiel

Les questions de responsabilité ne devraient pas constituer un frein au déploiement de la robotique de service. Elles seront traitées en grande partie par la jurisprudence dans le cadre de la loi du 19 mai 1998 sur la responsabilité du fait du produit défectueux.

[ISABELLE POTTIER](#)



TRANSACTION ET TRADUCTION FRANÇAISE D'UNE PREUVE ECRITE EN LANGUE ETRANGERE

La validité à titre de preuve d'un document écrit en langue étrangère

- La Cour de cassation rappelle les **règles générales de droit des contrats** et de procédure, concernant l'emploi de la langue française et la notion de transaction.
- L'Agence pour la sécurité de la navigation aérienne en Afrique et à Madagascar (ASECNA) a assigné une compagnie aérienne soudanaise en paiement de diverses factures.
- En 2007, le tribunal a fait droit à sa demande avec **exécution provisoire** (paiement de 3 580 867,95 euros majorée des intérêts de retard au taux de 6%). L'affaire ayant été **radiée du rôle** en 2008 (faute pour les parties d'avoir accompli les diligences procédurales qui leur incombaient), le conseiller de la mise en état a constaté la **péremption de l'instance**.
- La Cour d'appel de Paris a **confirmé** en décembre 2010, la péremption de l'instance, refusant de considérer que l'instance s'était précédemment éteinte par l'effet d'une transaction intervenue entre les parties.
- La société aérienne s'est **pourvue en cassation** reprochant à la cour d'appel d'avoir soumis des pièces de caractère non procédural à une exigence obligatoire de **langue française** et partant, de les avoir écartées, violant par là même l'ordonnance de Villers-Cotterêts d'août 1539 ainsi que l'article 6 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

Le défaut de traduction peut entraîner le rejet comme élément de preuve

- La Cour de cassation **rejette le pourvoi** de la compagnie aérienne, le 27 novembre 2012 (1).
- Elle considère que « *si l'ordonnance de Villers-Cotterêts d'août 1539 ne vise que les actes de procédure, le juge, sans violer l'article 6 de la CESDH est fondé, dans l'exercice de son pouvoir souverain, à écarter comme élément de preuve un document écrit en langue étrangère, faute de production d'une traduction en langue française* ».
- Par ailleurs, la société aérienne reprochait à la cour d'appel d'avoir déclaré **irrecevable une lettre** matérialisant l'accord des parties et constituant une transaction.
- La Cour de cassation rejette également cet argument. Elle considère qu'une lettre qui constitue une **mise en demeure de payer** « ne contient nullement les termes d'une transaction », car celle-ci « suppose l'existence de concessions réciproques des parties ».
- Même si elle entraîne un coût certain pour la partie qui le produit en justice, si l'une des parties souhaite produire en justice un document écrit en langue étrangère, il conviendra alors de s'assurer que cet acte soit accompagné d'une version traduite en français. A défaut, celui-ci pourra être **écarté par le juge**.
- Par ailleurs, il est rappelé que pour être qualifiée de transaction, l'acte de renonciation doit être subordonné à l'existence de **concessions réciproques** des parties.

Les enjeux

Un document écrit en langue étrangère peut-il constituer la preuve d'une transaction ?

(1) [Cass. com. 27-11-2012 n°11-17185](#).

Les conseils

La traduction en français d'un document écrit en langue étrangère est nécessaire pour éviter que celui-ci ne soit écarté par les juges.

Une mise en demeure qui ne comporte pas de proposition de règlement amiable par concessions réciproques ne peut être qualifiée de transaction.

[MARIE-ADELAÏDE DE MONTLIVALT-JACQUOT](#)
[ALEXANDRA MASSAUX](#)

Communications électroniques

TELECOMS ET LUTTE CONTRE LE TERRORISME

Où en est-on ?

- La loi du **21 décembre 2012** relative à la sécurité et à la lutte contre le terrorisme a été publiée au Journal officiel du 22 décembre 2012 (1).
- Considérant que la **menace terroriste demeure** à un niveau très élevé, ce texte vise à renforcer la répression contre le terrorisme, notamment lorsqu'il utilise des réseaux ou de services de télécommunications.
- Cette loi a notamment pour objet de **proroger, jusqu'au 31 décembre 2015**, les dispositions de l'article L 34-1-1 du CPCE, créé par l'article 6 de la loi 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers (2).
- La loi relative à la lutte contre le terrorisme fait suite à de nombreux textes législatifs traitant de la question de la **réétention des données de connexion**.
- La loi n° 2001-1062 du 15 novembre 2001 sur la sécurité quotidienne a soumis les opérateurs à l'obligation de conserver les données de leurs abonnés (art. 29, devenu art. L 34-1 du CPCE après modification par loi n° 2004-669 du 9-7-2004).
- Ce dernier dispositif de **conservation des données** avait été adopté pour une durée limitée (jusqu'au 31 décembre 2003), mais il a été finalement **pérennisé** par la loi n°2003-239 du 18 mars 2003 sur la sécurité intérieure.

Qui est concerné ? De quoi s'agit-il ?

- S'agissant de la **prévention des actes de terrorisme**, l'article L 34-1-1 du CPCE prévoit le cas des **réquisitions** administratives qui permettent aux agents de la police et de la gendarmerie nationales habilités à cet effet, à obtenir communication de **données conservées pendant un an** au titre de l'article L 34-1 du CPCE auprès des **opérateurs de communications électroniques** ou autres personnes fournissant un accès internet dans le cadre d'une activité professionnelle (exploitants de hotspots, tels que les cafés, les restaurants, les hôtels, les centres d'affaires, les cybercafés).
- Les obligations de conservation ne portent pas sur le contenu des communications échangées.
- Le cadre juridique a pour objet d'organiser les **modalités d'accès aux données** relatives au trafic (internet, géolocalisation, factures détaillées de téléphone), appelées également « données techniques de connexion », à savoir :
 - les informations permettant d'identifier l'utilisateur ;
 - les données relatives aux équipements terminaux de communication utilisés ;
 - les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
 - les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
 - les données permettant d'identifier le ou les destinataires de la communication ;
 - les données permettant d'identifier l'origine et la localisation de la communication.

Les enjeux

Lutter contre le terrorisme dans le respect des libertés individuelles.

(1) [Loi 2012-1432](#).

(2) Ces dispositions avaient déjà été reconduites par la loi 2008-1245 du 1-12-2008 visant à prolonger l'application des articles 3, 6 et 9 de la loi 2006-64 du 23-1-2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

L'essentiel

Prorogation, au-delà du 31 décembre 2012, des dispositions relatives à la lutte contre le terrorisme de la loi du 23 janvier 2006.

[FRÉDÉRIC FORSTER](#)

[EDOUARD LEMOALLE](#)



LES DONNEES D'IDENTIFICATION SUR INTERNET AU CŒUR DE L'ACTUALITE JUDICIAIRE

L'identification : prérequis pour définir la stratégie de réaction

- En matière de lutte contre les contenus ou comportements dommageables pour l'entreprise ou son e-réputation, l'**obtention des données d'identification** est souvent la première étape pour définir la stratégie de réaction appropriée et agir contre les auteurs des faits. L'anonymat et l'**usurpation d'identité** sont monnaie courante en la matière. Il n'est pas rare que le « client » qui clame son mécontentement sur un réseau social ou un forum soit en réalité le **concurrent direct**.
- Ces données d'identification ne peuvent être obtenues que sur **décision judiciaire**, auprès des prestataires techniques (hébergeurs de contenus ou FAI). La jurisprudence est venue lever certaines interrogations majeures en la matière.

Le cas du prestataire basé à l'étranger

- Il est possible d'obtenir du juge français qu'il ordonne la communication des données d'identification à un **hébergeur** basé à l'étranger, y compris aux Etats-Unis. Le Président du Tribunal de Grande instance de Paris a ainsi ordonné à Twitter de communiquer les **données d'identification des auteurs de tweets antisémites** (1), considérant que la **loi française était applicable**, les règles d'utilisation du site imposant aux utilisateurs de respecter les lois locales, et les contrevenants visés étant français (2).

Le cas du fournisseur d'accès

- Dans le cas où le détenteur des données est un **fournisseur d'accès**, les données d'identification peuvent également être obtenues par voie d'une **ordonnance sur requête**, sur le fondement de la LCEN.
- Dans une affaire concernant des demandes suspectes de transfert de noms de domaines, une société gérant des noms de domaine avait demandé qu'il soit ordonné à Bouygues Télécom la communication des données permettant d'identifier les abonnés correspondant aux adresses IP relevées.
- Le Président du TGI de Paris a fait droit à cette demande sur requête. Bouygues demandait cependant que cette ordonnance soit rétractée, faisant valoir que l'article [L34-1 du Code des postes et des communications électroniques](#) ne lui permettait de communiquer les données d'identification « *qu'exclusivement pour les besoins de la recherche, la constatation et la poursuite d'infractions pénales* ».
- Le juge a confirmé l'injonction de communiquer les données d'identification (3) en rappelant que les **FAI** sont des intermédiaires techniques **bénéficiant d'un régime de responsabilité atténuée** en vertu de la LCEN, « en contrepartie d'une obligation de conservation des données permettant d'identifier les personnes à l'origine d'un contenu », et **qui peuvent être requises par l'autorité judiciaire**.

Le cas de régies publicitaires et la nature des données

- L'exploitant d'un site internet avait constaté une baisse de ses revenus provenant de publicités AdSense et l'apparition de publicités inappropriées sur son site. Il a obtenu du Président du Tribunal de commerce de Paris qu'il ordonne à Google Ireland de lui communiquer l'identité des titulaires de comptes suspectés de détournement de revenus publicitaires, ainsi que **leurs coordonnées bancaires**, et les **montants versés** à leur profit (4).
- Cette décision obtenue sur requête a été confirmée en référé, Google Ireland ayant dans un premier temps refusé de s'exécuter. Le juge a considéré que l'obligation de communiquer les éléments n'était **pas sérieusement contestable**.

Les enjeux

Identifier l'auteur d'un contenu ou comportement litigieux est indispensable pour définir la stratégie de réaction et de réponse adéquate.

(1) [TGI Paris ord. réf. 24-1-2013](#).

(2) voir [JTIT n°132 février 2013, p.2](#)

Les conseils

Pour la victime des contenus : demander sur requête qu'il soit ordonné au prestataire technique de communiquer les données d'identification.

Pour les éditeurs de sites : se mettre en conformité avec les règles de collecte, de conservation et de communication des données d'identification.

(3) [TGI Paris ch. req. 30-1-2013](#).

(4) [TC Paris ord. réf. 1-2-2013](#).

[MATHIEU PRUD'HOMME](#)

[KATHARINA BERBETT](#)



LA REFORME DU E-COMMERCE : CE QUI ATTEND LES E-COMMERÇANTS

La directive 2011/83/UE relative aux droits des consommateurs

- Le 25 octobre 2011, l'Union européenne a adopté la directive n° 2011/83 relative aux droits des consommateurs qui harmonise et **complète les règles de protection** des consommateurs notamment en matière de vente à distance (1).
- La **transposition** de cette directive par les Etats membres doit intervenir d'ici au 13 décembre 2013, pour **entrer en vigueur au plus tard le 13 juin 2014**.
- L'objectif de cette harmonisation européenne est de **développer les ventes** transfrontalières à distance et notamment en :
 - diminuant les coûts de mise en conformité pour les professionnels ;
 - accroissant la confiance des consommateurs dans le marché intérieur ;
 - augmentant la sécurité juridique tant pour le consommateur que pour le professionnel.

Des évolutions imposant une revue des CGV et process de vente

- Cette **transposition** dans le droit français s'effectuera par une **loi** dont le projet a été annoncé par Benoit Hamon pour juin 2012.
- Ce texte imposera aux professionnels du e-commerce une **revue de leurs conditions générales en ligne**, des informations et présentation des produits et services sur le site ainsi que des process internes et logistiques pour prendre en compte les modifications législatives.
- Les **principales mesures** significatives pour les acteurs du e-commerce sont :
 - un renforcement de l'obligation d'information préalable du professionnel envers le consommateur tant au niveau du contenu (augmentation du nombre de mentions que de la forme en particulier lorsque la commande entraîne une obligation de payer ;
 - une extension du délai de rétractation à 14 jours au lieu de 7 jours et une variation des points de départ du délai en cas de livraisons multiples ;
 - l'introduction d'un modèle de formulaire de rétractation valable sur tout le territoire de l'Union européenne ;
 - des droits au remboursement plus étendus pour les consommateurs puisque l'intégralité de la somme y compris les frais de livraison sera à rembourser dans les 14 jours à compter de l'exercice du droit de rétractation ;
 - une obligation de rembourser le consommateur sur le même moyen de paiement que celui utilisé initialement sauf accord de celui-ci ;
 - une transparence plus grande sur les prix aussi bien s'agissant du coût total du produit que des frais supplémentaires mis à la charge du consommateur (frais de livraison, frais de retour le cas échéant, frais de services ajoutés) ;
 - une interdiction de recourir à des cases pré-cochées pour obtenir le consentement à tout paiement supplémentaire à la rémunération convenue au titre de l'obligation contractuelle principale
- Les **sanctions** prévues par les Etats membres en cas de non-respect de ces dispositions devront être « **effectives, proportionnées et dissuasives** ».

L'enjeu

Anticiper le nouveau référentiel e-commerce à venir

(1) [Directive 2011/83/UE du 25-10-2011](#).

Les conseils

- Identifier les impacts sur vos documents et process.

- Etablir un plan d'actions et un calendrier des modifications à effectuer tout en surveillant la transposition de la directive en droit interne.

[CELINE AVIGNON](#)

[AMANDINE POREE](#)



REFERENCEMENT PAYANT : NI CONTREFAÇON, NI CONCURRENCE DELOYALE ?

De la responsabilité alléguée du moteur de recherche...

- Par une décision du 29 janvier 2013, la Cour de cassation vient de rappeler les règles strictes permettant de poursuivre les moteurs de recherche dans le cadre de leur activité de référencement payant (1).
- Depuis les célèbres arrêts Google du 23 mars 2010 rendus par la Cour de justice de l'Union européenne, la responsabilité des moteurs de recherche apparaît en l'espèce soumise au **régime de responsabilité « allégé »** de la directive sur le commerce électronique, transposée en droit français au sein de la Loi du 21 juin 2004 sur la loi sur la confiance dans l'économie numérique, dès lors que, n'ayant pas joué un rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées (2).
- Dans l'affaire ayant conduit à l'arrêt du 29 janvier, la Cour d'appel avait néanmoins retenu la responsabilité du moteur de recherche au titre de la concurrence déloyale retenant que la société Google avait **techniquement contribué à la confusion générée** dans l'esprit du public en « proposant le mot-clé "Cobrason" dans le programme **Adwords** et en faisant ensuite apparaître sur la page de recherche s'ouvrant à la suite d'un clic sur ledit mot clé, sous l'intitulé "liens commerciaux", le site d'un concurrent à celui correspondant au mot-clé sélectionné ».
- La Cour de cassation **censure cette décision** qui retient la responsabilité du moteur de recherche sans avoir répondu aux conclusions de ce dernier qui revendiquait l'application du régime de responsabilité limitée des hébergeurs.

...à l'exigence de caractérisation de la faute de l'annonceur.

- Concernant la responsabilité de l'annonceur, la Haute cour se montre tout aussi stricte dans l'application de la règle de droit et notamment des conditions de mise en œuvre de l'action en concurrence déloyale
- Rappelant le **caractère licite du démarchage**, la Cour censure l'arrêt d'appel qui a retenu la faute de l'annonceur exerçant la même activité que le titulaire des droits sur le signe « cobrason » aux motifs qu'un tel usage aurait nécessairement généré une confusion entre les sites respectifs des parties. Il apparaît dès lors nécessaire de **caractériser les circonstances permettant de conclure à l'existence d'un risque de confusion** entre les sites internet des parties.
- Troisième et dernier point de cassation, la Cour **censure la décision** ayant retenu l'existence d'une publicité trompeuse au motif que l'internaute pourrait être porté à croire à l'existence d'un lien commercial particulier entre les sites des deux concurrents retenant que ces motifs sont « *impropres à caractériser une publicité fausse ou de nature à induire en erreur portant sur un ou plusieurs des éléments énumérés par l'article L. 121-1 du code de la consommation* » dans sa rédaction issue de la loi du 26 juillet 1993.
- Si la réforme de l'article L. 121-1 du Code de la consommation a abandonné la « publicité fausse ou de nature à induire en erreur » au profit de la « **pratique commerciale trompeuse** », les circonstances permettant de conclure à son existence demeurent limitativement définies.
- Il y a donc tout lieu de penser que la solution rendue au regard du nouveau texte eut été identique et que le référencement payant ne saurait constituer une **pratique commerciale trompeuse** sauf à **caractériser les circonstances limitativement visées par le Code de la consommation**.

L'enjeu

Empêcher le détournement de ses signes distinctifs par un concurrent sur les moteurs de recherche.

(1) [Cass. com. n°11-21011 et 11-24713](#), 29-1-2013.

(2) [CJUE, C236-08 à C238-08](#), 23-3-2010.

Les conseils

Analyser le contenu rédactionnel des annonces publiées dans le cadre d'un référencement payant.

Identifier les circonstances caractérisant un risque de confusion.

Identifier les circonstances caractérisant une pratique commerciale trompeuse.

[VIRGINIE BRUNOT](#)

[ANNE-SOPHIE CANTREAU](#)



CONTROLE FISCAL ET DONNEES CONSERVEES PAR LES OPERATEURS TELEPHONIQUES.

L'identité des émetteurs et destinataires de communications téléphoniques

- Pour les opérateurs de communications électroniques, la **conservation des données de connexion** est une obligation, rappelée tant par la loi du 21 juin 2004 pour la confiance dans l'économie numérique (**LCEN**) que par le Code des postes et communications électroniques (**CPCE**).
- En utilisant des informations relatives aux personnes émettrices et destinataires de communications téléphoniques, concernées par cette obligation de conservation, l'administration fiscale a pu démontrer l'existence d'une **fraude fiscale** dans le cadre de sa procédure de **visite et de saisie**, prévue à l'article L. 16 B du Livre des procédures fiscales (**LPF**).
- Cette affaire a, cependant, été portée devant les juridictions compétentes, puis, enfin, devant la Cour de cassation dans la mesure où les requérants soutenaient que les données à conserver et à traiter par les opérateurs ne peuvent porter sur l'**identification des interlocuteurs** des titulaires des lignes téléphoniques, conformément à l'article L. 34-1 V du CPCE.
- Ces mêmes requérants considéraient également que **seules les administrations** et les entreprises publiques pouvaient communiquer, sur demande de l'administration fiscale, les données conservées et traitées par les opérateurs de communications électroniques, conformément aux dispositions de l'**article L. 83 du LPF**.

L'administration fiscale peut demander communication de l'identité des clients des opérateurs

- De son côté, la Cour de cassation considère que l'administration fiscale peut demander **communication de l'identité des personnes** émettrices et destinataires.
- Elle a reconnu que les documents saisis dans le cadre de la procédure de visite et de saisie avaient une **origine licite** en rappelant que l'**article L. 34-1 V du CPCE** « *n'interdit que la conservation des données relatives au contenu des communications et que, parmi les catégories de données à conserver figurent celles portant sur l'identification des personnes utilisatrices du service* » (1).
- La Cour a ainsi estimé que, sans contrevenir aux dispositions de l'**article 8 de la Convention européenne**, l'article L. 34-1 V du CPCE autorise la conservation des données relatives aux personnes qui émettent une communication téléphonique et à celles qui en sont destinataires.
- La Cour de cassation en a ensuite déduit que les documents avaient une origine licite dans la mesure où les agents de l'administration fiscale ont exercé leur **droit de communication** sur le fondement de l'**article L. 85 du LPF**, lequel permet d'obtenir l'accès aux livres dont la tenue est obligatoire et des documents annexes, dont font précisément partie les **factures détaillées des opérateurs** de communications électroniques.
- Cette même Cour a ainsi **validé la démonstration, par l'administration fiscale**, de l'existence d'une fraude fiscale à partir des informations relatives aux personnes émettrices et destinataires de communications téléphoniques.

Les enjeux

La communication licite des données d'identification des interlocuteurs téléphoniques en matière de contrôle fiscal est-elle licite.

(1) [Cass. com 4-12-2012 n°11-27691](#).

Les conseils

Se souvenir que les factures détaillées de conversation téléphonique peuvent être communiquées à l'administration fiscale.

[PIERRE-YVES FAGOT](#)
[STEVE MOCHEE](#)



Indemnisation des préjudices

20 MILLIONS D'EUROS DE DOMMAGES ET INTERETS POUR DENIGREMENT

Propos dénigrants d'un opérateur mobile à l'égard de ses concurrents

- Le 15 janvier dernier, le Tribunal de commerce de Paris avait condamné la société Free Mobile à payer une somme de 400 000 euros à la société SFR (300 000 € de dommages et intérêts et 100 000 € de frais de procédure) pour dénigrement (1). Ce Tribunal a jugé en février une nouvelle affaire consécutive à l'entrée de Free sur le marché de la **téléphonie mobile** en janvier 2012 (2).
- Cette fois c'est Bouygues Télécom qui avait assigné Free, Free Mobile et Iliad, en leur reprochant le caractère agressif et dénigrant à son encontre de **campagnes de communication** lancées en janvier et septembre 2012 et de propos de leurs dirigeants, jugés très critiques à l'égard des autres opérateurs.
- Considérant le caractère particulièrement violent et injurieux des propos tenus à l'égard des concurrents, le Tribunal condamne le titulaire de la quatrième licence et ses filiales pour **actes de dénigrement** constitutifs de **concurrence déloyale** et leur interdit d'utiliser le champ lexical utilisé et notamment les termes « arnaque », « racket » et « escroquerie », **sous astreinte de 100 000 euros** par infraction.
- En réparation de son **préjudice moral et économique**, Bouygues Télécom demandait une indemnisation de **98,8 millions d'euros**, estimant avoir subi une **perte de clientèle** et une **atteinte à son image**.
- Free formulait reconventionnellement des demandes de réparation, également pour **dénigrement**, d'un montant, probablement fixé volontairement, et peut être arbitrairement, à un niveau à peine supérieur, de **99 millions d'euros**.

Evaluation souveraine, et peu documentée, des préjudices

- Bouygues Télécom considère que l'entrée de Free sur le marché lui a fait perdre 1 million de clients, mais un expert judiciaire a chiffré à **181 106 la perte de clients** liée **uniquement au dénigrement**, chiffre retenu par le jugement.
- Le jugement retient ensuite une « **valorisation** » de **357 € par abonné**, soulignant que la formule de calcul de cette valeur ne serait pas spécifique à Bouygues Télécom, mais une « formule mathématique standard de calcul de Valeur Actuelle Nette », tenant compte de la marge par abonné, du « churn » et du taux d'actualisation, mais sans préciser les méthodes ni les hypothèses de calcul de ces données, qui sont pourtant propres à chaque opérateur et discutables.
- Le nombre de clients perdus (181 106) et la « valeur » d'un client (357 €) **retenus** auraient donné un montant de 64 654 852 euros, mais le jugement use de son « pouvoir d'appréciation » et chiffre le préjudice causé par la perte de clientèle à **15 millions d'euros** (soit **82,82 € par client**) sans autre précision.
- Constatant que Bouygues Télécom doit engager des **dépenses** de communication pour rétablir son image et relevant que Free évalue son préjudice d'image à 25 100 000 euros, le jugement chiffre le **préjudice d'image** de Bouygues Télécom à **10 millions d'euros**.
- Bouygues Télécom ayant également communiqué au sujet de Free et en réponse à ses critiques, de manière virulente, le jugement retient également des **actes de dénigrement** à son encontre. Relevant que Free accepte la méthode d'évaluation retenue pour chiffrer le préjudice de Bouygues Télécom, le jugement chiffre à 48 440 clients la perte de clientèle de Free et son préjudice à **5 millions d'euros** (soit **103,22 € par client**) sans fournir le détail des calculs effectués.

Les enjeux

Les enjeux économiques et sociaux de ces affaires sont considérables puisqu'ils se chiffrent en millions d'euros et ne sont pas neutres en matière d'emploi. Or, les décisions donnent peu de détail sur l'évaluation des préjudices

(1) T Com Paris 15-1-2013, [RG 2012-033422](#).

(2) T Com Paris 22-2-2013, [RG 2012-076280](#).

Les conseils

Il serait donc souhaitable que les débats gagnent en profondeur sur l'évaluation des préjudices et que ceci soit reflété dans la transparence des motivations des décisions sur le montant des préjudices. Même si les juges du fond apprécient souverainement l'étendue des préjudices, ils doivent aussi veiller à leur réparation intégrale, sans perte ni profit pour les parties.

[BERTRAND THORE](#)



ACTUALITE DROIT SOCIAL NUMERIQUE

Références

TéléRC : service en ligne d'homologation de rupture conventionnelle

- Créée par la loi du 25 juin 2008, la **rupture conventionnelle** connaît depuis lors un succès massif avec plus de 260 000 demandes homologuées sur la seule année 2012.
- Si en 2008, 12 % des demandes étaient jugées irrecevables et 21 % de celles recevables rejetées, en 2012, le nombre de **demandes jugées irrecevables chute à 2 %** et le nombre de celles **rejetées à 6 %** alors que leur nombre ne cesse de croître.
- C'est dans l'optique de **réduire au maximum les risques** d'irrecevabilité et de refus, que le Ministère du Travail a instauré, le 1^{er} février 2013, un portail internet d'homologation des demandes de rupture conventionnelle (1).
- Ce service permet de s'assurer que les mentions obligatoires sont remplies, les délais légaux respectés et l'indemnité de rupture au moins égale au minimum légal. Le **traitement** par l'administration en est **facilité et accéléré**.
- Une fois le formulaire rempli, il suffit de l'imprimer en 3 exemplaires, signés par l'employeur et le salarié, puis de l'envoyer, à l'issue du délai de rétractation de 15 jours calendaires prévu par la loi, à la direction régionale des entreprises, de la concurrence, de la consommation du travail et de l'emploi (DIRECCTE).
- A noter que cette procédure en ligne n'est **pas applicable aux salariés protégés** qui bénéficient d'une procédure particulière avec demande d'autorisation auprès de l'inspection du travail.

(1) Formulaire sur
www.telerc.travail.gouv.fr

Utilisation abusive de la messagerie professionnelle et licenciement

- « *il a ainsi utilisé la messagerie professionnelle et, quoi qu'il en dise, a ainsi distraité une partie non négligeable de son temps (même si les messages pour sa société n'étaient pas très longs, il devait réfléchir à la réponse à faire) à des fins extérieures à son activité.* ».
- C'est ainsi que la Cour d'appel d'Orléans, dans sa décision du **29 janvier 2013**, a retenu que le comportement du salarié justifiait un licenciement sans cause réelle et sérieuse (2).
- Dans les faits, la **charte informatique** de la société spécifiait que la messagerie des salariés était à vocation exclusivement professionnelle et le règlement intérieur interdisait le travail personnel au sein des locaux de l'entreprise.
- En dépit de cette **double interdiction**, le salarié en cause a fait un usage personnel de sa messagerie professionnelle, certains de ces méls ayant par ailleurs pour objet son **activité extérieure** en tant que co-gérant d'une société. Le salarié a donc été licencié pour « *détournement de moyens professionnels à usage personnel* ».
- On peut néanmoins se questionner sur l'articulation de la décision avec la notion de **vie privée résiduelle**. Dans quelle mesure l'utilisation personnelle de l'outil de messagerie professionnelle est-elle constitutive d'un abus justifiant un licenciement sans cause réelle et sérieuse ?
- Si un « abus » est caractérisé en l'espèce, quelle est la limite quantitative et/ou qualitative d'envoi/réception de mél personnel *via* une messagerie professionnelle au-delà de laquelle le licenciement sans cause réelle et sérieuse se justifie ?

(2) [CA Orléans, 29-1-2013, n° 11/03345](#).

[EMMANUEL WALLE](#)
[ANNE ROBINET](#)
[NAOMI SUCHOD](#)



Prochains événements

Escroqueries sur internet : Quelles stratégies de lutte ? Quels plans de réduction du risque ? : 13 mars 2013

- **Virginie Bensoussan-Brulé**, animera au côté de **Luc Alloin**, fondateur et dirigeant de [Securymind](#), cabinet de conseil expert en stratégies de protection, un petit-déjeuner débat consacré aux stratégies et plans de réduction du risque en matière d'escroqueries sur internet.
- Jusque-là relativement épargnées, les entreprises françaises sont la cible, depuis quelques mois, d'une recrudescence d'escroqueries à grande échelle sur internet utilisant leur dénomination sociale, leur logo, leur marque ou encore leur nom de domaine.
- D'une infraction à l'autre, le mode opératoire est peu ou prou le même. Les internautes (particuliers, fournisseurs, etc.) sont destinataires d'un courrier électronique ou d'une annonce au nom de la société leur proposant matériels ou offres d'emploi en échange du paiement d'une certaine somme. La somme une fois acquittée, ils n'ont bien sûr, aucun retour sur investissement.
- Tout est orchestré pour que l'internaute n'ait aucun doute sur la provenance de la proposition frauduleuse : utilisation du logo de la société, extension d'adresse de courrier électronique, utilisation de fausses identités présentées comme dirigeants ou salariés de l'entreprise et, parfois même, création d'un faux site internet.
- Face à ces comportements malveillants, les sociétés ne sont pas pour autant démunies. De nombreuses mesures leur permettent de lutter efficacement contre ces atteintes à leur réputation et à leur droit de propriété intellectuelle.
- Nous vous proposons d'étudier ces procédures de suppression, identification et répression lors d'un petit-déjeuner débat.
- **Inscription gratuite** sous réserve de confirmation avant le 8 mars 2013 en renseignant le [formulaire en ligne](#).

Groupe de travail sur un livre blanc « Vidéoprotection » : 1^{ère} réunion le 5 avril 2013

- Le régime juridique de la vidéoprotection a été profondément modifié depuis la Loppsi 2 : nouvelle terminologie, extension des possibilités d'y recourir, conditions de visionnage des images par des agents privés assouplies, nouvelles garanties, nouvelles responsabilités, etc.
- Les membres du [GPMSE Installation](#) (Groupement professionnel des métiers d'installateurs mainteneurs en sécurité électronique), les équipes de [AASSET Sécurité-TKH](#) et **Alain Bensoussan** souhaitent apporter un regard multisectoriel et pluridisciplinaire sur ces problématiques à travers la rédaction d'un livre blanc.
- Ce **Livre Blanc** s'adresse à tous ceux qui veulent prendre la mesure des responsabilités liées à la vidéoprotection, et qui, au-delà des seuls aspects techniques, veulent aussi prendre en compte les aspects juridiques associés.
- Par la diffusion de ce Livre Blanc, nous souhaitons participer à une meilleure compréhension par tout un chacun des réalités de la vidéoprotection et faire en sorte que la « sécurité » reste le maître mot des utilisateurs.
- Son objectif est de faciliter le travail des acteurs du marché de la vidéoprotection et des utilisateurs à chacun de leur niveau d'implication (dirigeants, collaborateurs et service informatique gérant les dispositifs de vidéoprotection, prestataires), tout en permettant un dialogue entre ces diverses populations autour de ce sujet.
- Ce Livre Blanc paraît particulièrement opportun à l'approche de la réforme du livre VI du code de la sécurité intérieure, CSI, texte fondateur pour le secteur de la sécurité privée.
- La **première réunion** se tiendra le 5 avril 2013 (8h30/10h30) dans [nos locaux](#).
- Les prochaines réunions du groupe de travail s'articuleront autour des thématiques suivantes :
 - 3 mai : les précautions à prendre lors de l'installation d'un dispositif de vidéoprotection ;
 - 14 juin : le masquage des zones privées ;
 - 6 septembre : les personnes habilitées à visionner les images enregistrées ;
 - 11 octobre : la reconnaissance faciale et les systèmes biométriques associés à un dispositif de vidéoprotection
 - 6 novembre : les durées de conservation des images ;
 - 6 décembre : le rôle d'accompagnement des installateurs et les outils appropriés d'information.
- **Inscription gratuite** sous réserve de confirmation avant le 2 avril 2013 par courrier électronique en indiquant vos coordonnées et le nombre de personnes qui assisteront au petit déjeuner débat à l'adresse suivante : invitation-conference@alain-bensoussan.com ou en faxant le [bulletin d'inscription](#) en ligne au 01 41 33 35 36.



NOTRE RESEAU DE CORRESPONDANTS ORGANIQUES LEXING VOUS INFORME

Affaire Onel : la notion d'usage sérieux d'une marque communautaire précisée

- La protection d'une marque est limitée en vertu du principe de territorialité, de sorte que les droits de son titulaire ne s'étendent pas au-delà du territoire pour lequel la protection a été demandée. Par rapport à cette restriction aux droits du titulaire, la [marque communautaire](#) (1) peut constituer une solution intéressante.
- Dans le cadre d'un différend relatif à l'enregistrement comme marque Benelux d'un signe « OMEL » présentant de fortes ressemblances avec une marque communautaire antérieure « ONEL », une juridiction néerlandaise a interrogé la Cour de Justice européenne sur la **notion d'usage sérieux** d'une marque communautaire compte tenu du fait qu'en l'espèce, la marque communautaire « ONEL » n'était utilisée qu'aux Pays-Bas.
- Dans un arrêt du **19 décembre 2012** ([aff. C-149/11](#)), la Cour de Justice européenne a répondu à la juridiction néerlandaise en apportant des précisions fondamentales sur la notion d'usage « sérieux » d'une marque communautaire.

Afrique du Sud : le projet de loi sur la protection des renseignements personnels bientôt promulgué

- Le projet de loi sur la protection des renseignements personnels en Afrique du Sud ([POPI-BILL-9B-OF-2009 \(EN\)](#)) fait lentement son chemin.
- Le **13 février 2013**, le Comité spécial sur la sécurité et le développement constitutionnel (un comité du NCOP) s'est réuni sur le POPI (*Protection of Private Information Bill*).
- Il doit encore être modifié pour tenir compte de la législation européenne sur la protection des données.
- Le Comité doit se réunir **courant mars** pour arrêter la version du projet de loi qui sera soumise à l'Assemblée nationale pour adoption fin mars. Le projet de loi **pourrait être promulgué en Afrique du Sud cette année**.

Envoyer des emails en copie masquée peut coûter cher

- Envoyer un email à plusieurs destinataires sans cacher les adresses des interlocuteurs (en utilisant le **champ « Cci »**), de sorte que chaque destinataire peut obtenir les adresses électroniques des personnes et vice versa, est une **violation** grave de la loi sur la protection des données.
- En cas de plainte à l'Agence espagnole de protection des données (AEPD), le contrevenant s'expose à des sanctions financières pouvant aller de de **40 000 à 300 000 euros** selon que les données ont été obtenues légalement, le nombre de destinataires ne dépasse pas 1000 et le type d'informations contenues dans le message n'est pas particulièrement sensible (1).

Du nouveau sur la réglementation des eFactures

- Le règlement sur la facturation électronique en vigueur depuis le **1er janvier 2013**, propose une nouvelle définition de la facturation électronique pour tenir compte de la neutralité technologique (2).
- Elle peut être émise ou reçue dans **n'importe quel format** (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg ou txt, etc.) dès lors que l'authenticité et l'intégrité du document sont garanties.



Lexing Belgique

[Philippe & Partners](#)

Newsletter [IP, IT & TMT 09](#) du 18-2-2013



Lexing Afrique du Sud

[Cabinet Michalsons](#)

[Actualité](#) du 20-2-2013.



Lexing Espagne

[Cabinet Alliant](#)

(1) [Actualité](#) du 23-2-2013.

(2) [Actualité](#) du 2-2-2013.



Protection des données personnelles : le plan d'action des Cnil européennes

- Google est menacé d'une **action répressive** par les autorités européennes de protection des données pour sa politique de confidentialité.
- N'ayant pas obtenu de réponse à ses recommandations dans le délai fixé, le groupe des autorités européennes a publié un communiqué de presse daté du **27 février 2013** (1) dans lequel il annonce la création d'un groupe de travail piloté par la Cnil pour coordonner une action répressive envers Google **avant l'été**.

(1) [Communiqué G29 Google privacy policy \(EN\) du 27-2-2013.](#)

Recommandations de sécurité de l'ANSSI sur les dispositifs de vidéoprotection

- Les recommandations formulées par l'ANSSI visent à **contrer les vulnérabilités** potentielles ou du moins à en limiter l'impact.
- Elles portent sur l'ensemble des composants d'un dispositif de vidéoprotection : déploiement physique des capteurs, architecture du réseau support, configuration des équipements et du centre de supervision (2).

(2) [Doc ANSSI n° 524 du 14-2-2013.](#)

Le gouvernement souhaite relancer les espaces publics numériques

- **5000 EPN** présents sur l'ensemble du territoire dont 2500 adhèrent au label NetPublic, coordonné par la Délégation aux Usages de l'Internet (DUI).
- Ces espaces permettent de sensibiliser et d'accompagner les citoyens dans l'appropriation des usages du numérique. La ministre a insisté sur les **évolutions** que ces structures doivent aujourd'hui engager pour répondre à des besoins socio-économiques et culturels nouveaux (3).

(3) [Communiqué du 19-2-2013.](#)

Proposition de directive sur la sécurité des réseaux et de l'information

- Le 7 février 2013, la Commission européenne a publié la stratégie de l'Union européenne en matière de **cybersécurité** (4), ainsi qu'une proposition de directive concernant la **sécurité des réseaux** et des **systèmes d'information** (5).

(4) [CE, Communication du 7-2-2013 \(EN\).](#)

(5) [COM \(2013\) 48 final du 7-2-2013.](#)

Révision des lignes directrices sur les aides d'Etat du secteur du haut débit

- De nouvelles lignes directrices communautaires 2013/C 25/01, pour l'application des règles relatives aux aides d'Etat dans le cadre du déploiement des réseaux de communication à haut débit, ont été publiées le **26 janvier 2013** (6).
- Elles prévoient, notamment un renforcement des obligations de libre accès, l'autorisation des interventions publiques là où le marché est défaillant et des règles de transparence améliorées.

(6) [Communication du 26-1-2013.](#)

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/ouils/abonnement-juristendance>

©Alain Bensoussan 2012



Formations intra-entreprise : 1^{er} semestre 2013

Le cabinet a la qualité d'organisme de formation professionnelle depuis 30 ans¹.

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 30-05-2013

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



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

▪ 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](#).



[Informatique,](#)
[Télécoms, Internet,](#)
Editions Francis
Lefebvre 5e éd. 2012

² Nos publications : <http://www.alain-bensoussan.com/espace-publication/bibliographie>