

La LCEN fête ses un an !

Une jurisprudence « responsabilisante » ...

▸ La loi pour la confiance dans l'économie numérique ⁽¹⁾ fête ses un an d'existence, occasion rêvée pour en tirer un **premier bilan**.

▸ Un an de jurisprudence essentiellement axée sur la problématique de la **responsabilité des acteurs de l'internet** qui, à leur corps défendant, voient leurs obligations croître et leurs responsabilités enfler.

▸ A titre d'exemple, la condamnation pour faute d'un **hébergeur** qui enregistre des coordonnées fantaisistes ne permettant pas l'identification de l'auteur d'un site litigieux ⁽²⁾ ou encore l'attribution de la qualité de **prestataire technique** à une entreprise, l'obligeant ainsi à conserver les données de connexion de ses employés afin de les communiquer sur réquisitions judiciaires ⁽³⁾.

▸ La jurisprudence permet aussi de confirmer que **les grands oubliés** de la LCEN ⁽⁴⁾ rencontrent des difficultés plus grandes encore, par exemple les régies publicitaires et moteurs de recherche à propos de la pratique des liens sponsorisés et du positionnement payant sur internet ⁽⁵⁾.

Une loi de « sanction » qui risque d'évoluer ...

▸ Sur l'ensemble des **décrets** attendus, seul le décret sur les conditions d'**archivage des contrats « clic »** a été arrêté et renforce ici les obligations des cyber-commerçants ⁽⁶⁾.

▸ Le point positif du bilan est sans nul doute la prise de **position de la Cnil** qui limite la portée des dispositions relatives à la **prospection par voie électronique**, aux seules prospections de type B to C.

▸ Alors même que le cadre juridique fête son premier anniversaire le 21 juin et malgré la jurisprudence toujours plus « responsabilisante », il faut constater que trop peu d'entreprises sont dans une **démarche de mise en conformité**.

▸ Ceci est d'autant plus imprudent que la LCEN est une loi de sanction où la seule absence de « **notice légale** » est punie d'un an de prison et de 75 000 euros d'amende.

▸ On ne peut qu'inciter les entreprises à s'engager dans cette voie d'autant plus indispensable que la LCEN I cèdera nécessairement la place à une **LCEN II** du fait de la **modification prochaine** de la directive communautaire sur le commerce électronique (à l'origine de la loi française). L'acquisition des compétences s'avèrera donc **plus compliquée**.

L'enjeu

Créer un statut spécifique au commerce en ligne afin de diminuer l'insécurité juridique

(1) Loi n° 2004-575 du 21/06/2004.

(2) TGI Paris, 16/02/2005 Tiscali.

(3) CA Paris, 04/02/2005, BNP Paribas.

(4) Cf. l'interview de Stéphane Marcovitch (AFA), p.10 ci-après.

(5) TGI Nanterre, 17/01/2005, Sté Overture ; TGI Paris, 04/02/2005, Stés Google inc et Google France.

Le conseil

- entamer une démarche de mise en conformité à la LCEN (déclarations Cnil, notice légale...);

- suivre les travaux de modification de la directive CE afin de préparer la LCEN II.

(6) Décr. n° 2005-137, JO du 18/02/2005.

EricBarbry,
eric-barbry@alain-bensoussan.com

Informatique

La fraude informatique et le nouveau délit de détention de virus

Détenir des virus est interdit ...

▸ Le nouvel **article 323-3.1 du Code pénal** inséré par la loi du 21 juin 2005 réprime l'importation ou la détention, l'offre, la cession ou la mise à disposition de tout équipement, instrument ou programme informatique ou encore donnée conçue ou spécialement adaptée pour la commission d'une infraction relevant des atteintes aux systèmes de traitement automatisé de données traditionnellement réprimées par le dispositif législatif issu de la **loi « Godfrain »**.

▸ Le but poursuivi par le législateur est de ne plus avoir à attendre la commission des infractions liées à l'atteinte aux systèmes informatiques pour réprimer le fraudeur puisque désormais, il suffit de **détenir des codes sources** ou encore des données, conçues ou spécialement adaptées à la fraude informatique pour risquer une condamnation pouvant aller jusqu'à **5 ans de prison** et/ou **75 000 euros d'amende**.

▸ Si le dispositif permet la **falsification de chèques** ou de cartes de paiement, le **risque** est **aggravé** en application des dispositions du Code monétaire et financier qui répriment spécifiquement ce type d'infraction. La méfiance est de mise, même si posséder n'est pas (toujours) frauder.

... sauf motif légitime

▸ Selon la **convention sur la cybercriminalité**, l'obtention ou la mise à disposition des dispositifs incriminés n'est pas répréhensible dès lors qu'il ne s'agit pas de commettre une infraction par exemple dans le cas d'**essais autorisés** ou de **protection d'un système informatique**.

▸ Le Code pénal français indique pour sa part que la **détention** de tels dispositifs peut se trouver justifiée par un « **motif légitime** ».

▸ C'est donc au juge éventuellement saisi, d'apprécier la légitimité de la **détention d'un virus informatique** et bien qu'aucune décision de justice n'ait été à ce jour prononcée sur ce fondement, on peut imaginer, en prenant pour exemple la convention sur la cybercriminalité que ne serait pas réellement inquiétés les services informatiques des entreprises qui possèdent dans des **environnements sécurisés** de tels virus afin d'**expérimentation des dispositifs de prévention**.

▸ Le principe en matière pénale est qu' «il n'y a point de crime ou de délit sans intention de le commettre». La charge de la preuve du motif légitime incombera aux possesseurs du virus. Il ne faut donc pas hésiter à se prémunir de toute détention d'un virus qui ne serait pas justifiée.

L'enjeu

Réduire les risques en mettant en œuvre des procédures adéquates et réserver la détention des dispositifs incriminés aux services informatiques spécialisés aux seules fins de la politique de prévention contre les risques informatiques.

Les conseils

- Mettre à jour la charte informatique en rappelant l'interdiction stipulée à l'article L 323-3-1 du Code pénal et les sanctions associées. ;
- Disposer d'une procédure en cas de détention des dispositifs incriminés par la loi, en considération des objectifs légitimes poursuivis.

Jean-François Forgeron
jean-francois-forgeron
@alain-bensoissan..com

Communications électroniques

L'obligation de conservation des logs de connexion : nous sommes tous des FAI !

Détenir et de conserver les données de connexion des utilisateurs

▸ La loi du 9 juillet 2004 (dite « Paquet télécom ») qui a profondément modifié le Code des postes et des communications électroniques, combinée aux dispositions de la loi pour la confiance dans l'économie numérique du 21 juin 2004 fixe des règles extrêmement fortes s'agissant de **l'identification des éditeurs de services en ligne** d'une part, et de la **conservation des logs de connexion** pendant une durée d'un an (obligation issue de la loi du 1er août 2000) d'autre part.

▸ La loi pour la sécurité quotidienne du 1er août 2000 impose en effet aux FAI «*de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu*» de services dont ils sont prestataires (art. 43-9).

▸ Cette obligation a précisément été instaurée afin de **faciliter le travail des enquêteurs de police** en cas de contenus illicites.

Faciliter le travail des enquêteurs de police

▸ La **Cour d'appel de Paris**⁽¹⁾ a précisé qu'une **entreprise** qui met à disposition de ses **salariés** des connexions internet doit être considérée comme un **prestataire internet** et plus précisément un fournisseur d'accès.

▸ La cour a ainsi obligé l'entreprise à fournir tous les éléments d'information à sa disposition permettant l'identification de l'expéditeur d'un **message anonyme litigieux** envoyé à partir d'un poste installé dans ses services.

▸ Se faisant, elle précise que les **contours de l'obligation** issue de la loi du 1er août 2000 n'imposent pas à l'entreprise de traiter les données, cette dernière doit seulement **conserver et communiquer**, et non procéder elle-même à l'identification de l'expéditeur, ceci ne pouvant relever que d'une mesure d'instruction judiciaire.

▸ Cette jurisprudence implique l'obligation pour toutes les entreprises de mettre en place des outils permettant l'identification des utilisateurs (**logiciels de filtrage**) et la conserver les logs de connexion pendant un an afin de les tenir à disposition de la police.

L'enjeu

Préserver le droit à l'anonymisation des communications et au secret absolu de leur contenu tout en assurant la sécurité sur internet.

Les conseils

Mettre en place des outils permettant :

- l'identification des utilisateurs ;
- la conservation pendant un an des logs de connexion.

(1) CA Paris, 04/ 02/ 2005, BNP Paribas.

Eric Barbry,
eric-barbry@alain-bensoussan.com

Collectivités territoriales

Le juge donne le contour des nouvelles compétences des collectivités issues de la LCEN

Un droit d'intervention en matière de communications électroniques

▸ La loi du 21 juin 2004 pour la confiance dans l'économie numérique a inséré dans le Code général des collectivités territoriales l'article L 1425-1 qui autorise les collectivités territoriales à **établir** et **exploiter** un **réseau de communication électronique** dès lors que l'insuffisance de l'initiative privée est constatée.

▸ Les modalités d'application de cet article sont précisées dans la **circulaire ministérielle** du 21 janvier 2005 ⁽¹⁾.

▸ Les collectivités peuvent mettre en œuvre leurs nouvelles compétences dans le cadre d'une convention de **délégation de service public (DSP)** ou d'un **marché public**.

▸ Par ailleurs, la Commission européenne approuve le **financement public** dès lors qu'il constitue « *la compensation d'une obligation de service d'intérêt économique général* » et non une aide d'Etat ⁽²⁾.

Le respect du principe d'égalité et de libre concurrence

▸ Les collectivités territoriales doivent néanmoins respecter les principes de mise en concurrence si elles ne veulent voir leurs **projets sanctionnés**.

▸ Ainsi, à la demande de l'association de contribuables de l'Hérault (ACH), le tribunal administratif de Montpellier ⁽³⁾ a ordonné en référé, la **suspension d'une délibération** du Conseil général de l'Hérault accordant une subvention de 25 millions d'euros pour l'établissement et l'exploitation d'un réseau départemental de communications électroniques à haut débit.

▸ La procédure d'attribution de la délégation de service public (DSP) à un opérateur de communications électroniques a été **déclarée irrégulière** pour **information insuffisante** des conseillers généraux suite au changement substantiel du financement du projet.

▸ Il a également relevé un manquement grave du Conseil général au **principe d'égalité des candidats** du fait de l'attribution d'une aide publique généreuse « *au seul candidat qu'il voulait manifestement choisir* ». Le Conseil Général de l'Hérault a toutefois décidé de porter cette décision devant le Conseil d'Etat.

L'enjeu

Renforcer les capacités d'intervention des collectivités en matière d'aménagement numérique de leur territoire.

(1) www.telecom.gouv.fr/

(2) Déc. CE du 03/05/2005 (IP/05/530) Limousin et déc. CE du 16/11/2004 (IP/04/1371) Pyrénées Atlantiques disponibles sur [//europa.eu.int](http://europa.eu.int)

Les conseils

- Constater l'insuffisance d'initiative privée par un appel d'offres déclaré infructueux ;

- Informer l'Autorité de régulation des télécommunications ;

- Veiller à ne pas générer de pratique anticoncurrentielle.

(3) TA Montpellier, Ord. réf. 01/04/2005 n^{os} 0501218/0501219.

Danièle Véret
danièle-veret@alain-bensoussan.com

Propriété intellectuelle

Le renforcement des sanctions pour les infractions commises sur les services en ligne

Elargir les pouvoirs du président dans les saisies contrefaçon

▸ L'article 8 de la loi pour la confiance dans l'économie numérique du 21 juin 2004 a introduit dans le Code de la propriété intellectuelle (CPI) de **nouvelles dispositions** concernant la saisie contrefaçon.

▸ Cet article étend les pouvoirs du Président du tribunal de grande instance, statuant par ordonnance sur requête, selon la **procédure spécifique** de saisie contrefaçon. En effet, celui-ci a désormais la faculté de suspendre «*par tout moyen le contenu d'un service de communication publique en ligne portant atteinte à l'un des droits de l'auteur, y compris en ordonnant de cesser de stocker ce contenu ou, à défaut, de cesser d'en permettre l'accès*». Cet article **confirme la jurisprudence** qui montre que les juges recouraient déjà à cette faculté (1).

▸ La loi précise que dans ce cas d'application de la procédure de saisie contrefaçon, le **délai de mainlevée** prévu à l'article L. 332-2 du CPI est **réduit à 15 jours** (au lieu de 30).

▸ Elle permet aussi au tribunal d'ordonner en cas de condamnation pour contrefaçon, aux frais du condamné, la **publication** intégrale ou par extrait du jugement **sur les services de communication publique en ligne**.

▸ Enfin, les **titulaires de droits voisins** tout comme les auteurs ont accès aux procédures, civiles et pénales en matière de saisie contrefaçon. Sont ainsi concernés les artistes interprètes, les producteurs de phonogrammes et vidéogrammes et les entreprises de communication audiovisuelle.

Une première application jurisprudentielle

▸ Les juges ont fait une des premières application de l'article 8 de la loi LCEN applicable **en matière de droits voisins**, par une ordonnance rendue sur requête du 8 octobre 2004⁽²⁾.

▸ En l'espèce, les requérants souhaitaient obtenir la résiliation du contrat d'accès au site internet au titre des dispositions générales de l'article 61-8 de la loi du 21 juin 2004 (ordonnance sur requête).

▸ Le président a **rejeté la requête** au motif que «*la résiliation d'une convention permettant l'accès à internet ne ressort pas de la compétence du juge des requêtes ni de celle du juge des référés*».

▸ L'ordonnance précise qu'il convient dans ce cas d'appliquer l'article 8 de la LCEN pour obtenir la **suspension d'accès au site**, les dispositions qu'il contient paraissant mieux adaptées à la situation de l'espèce.

L'enjeu

Donner plus d'efficacité aux actions notamment lorsque les éditeurs de sites sont difficiles à identifier ou à atteindre.

(1) TGI Lille Ord. réf., 17/09/2002 Association Taroteam c. Thierry A., SA Free, Jeanne P.

Les conseils

- Demander la mise en ligne de tout ou partie du jugement ;

- Bien cibler son action et demander une suspension et non une résiliation du contrat d'accès internet.

(2) TGI Paris, 3ème ch., Ord. sur requête, 08/10/2004.

Laurence Tellier-Loniewski
Florence Revel de Lambert
laurence-tellier-loniewski@alain-bensoussan.com

Relations sociales

La vidéosurveillance des locaux de l'entreprise ⁽¹⁾

▸ Dans un arrêt en date du 19 avril 2005, la Chambre sociale de la cour de Cassation s'est de nouveau prononcée sur l'admissibilité de **preuves par enregistrements vidéos** à propos de quatre salariés engagés par une société en qualité d'agents de surveillance **licenciés pour faute grave**.

▸ Le Conseil de Prud'hommes et la cour d'appel ont retenu les bandes vidéos comme moyen de **preuve licite** établissant l'existence de la faute grave.

▸ La Chambre sociale de la cour de Cassation réaffirme le principe interdisant la mise en œuvre d'un dispositif de contrôle de l'activité professionnelle n'ayant pas été **porté préalablement à la connaissance des salariés** mais indique qu'il peut être opposé aux salariés des preuves recueillies par un système de **surveillance des locaux** auxquels ils n'ont pas accès.

▸ S'agissant d'un prestataire, l'employeur n'est pas tenu de divulguer l'existence des **procédés installés par les clients de l'entreprise**. En l'espèce, la mise en place de la caméra avait été décidée par un client et n'avait pas pour but de contrôler le travail des salariés mais uniquement de **surveiller la porte d'accès** d'un local dans lequel il ne devait y avoir aucune activité, et que les enregistrements vidéos litigieux constituaient un moyen de preuve tout à fait licite.

L'extrait

« Mais attendu (...) qu'ayant constaté que la mise en place de la caméra avait été décidée par un client et n'avait pas pour but de contrôler le travail des salariés mais uniquement de surveiller la porte d'accès d'un local dans lequel il ne devait y avoir aucune activité, la Cour d'appel a pu décider, sans encourir les griefs du moyen, que les enregistrements vidéos litigieux constituaient un moyen de preuve licite ; que le moyen n'est pas fondé ».

(1) Cass. soc. 19 avril 2005.

Le contrôle des fichiers informatiques du salarié ⁽²⁾

▸ Un dessinateur a été **licencié pour faute grave** aux motifs qu'à la suite de la découverte de photos érotiques dans un tiroir de son bureau, il avait été procédé à une **recherche sur le disque dur** de son ordinateur qui avait permis de trouver un ensemble de dossiers totalement étrangers à ses fonctions, figurant notamment dans un **fichier intitulé « perso »**.

▸ La cour d'appel a validé le licenciement fondé sur une faute grave en considérant que la **découverte des photos érotiques** n'ayant aucun lien avec son activité constituait des circonstances exceptionnelles autorisant le contrôle du **contenu du disque dur de l'ordinateur**. En outre, il n'y avait **aucun code personnel** attribué au salarié pour empêcher une autre personne que l'utilisateur d'ouvrir les fichiers.

▸ La cour de Cassation reste très ferme et considère que **sauf risque ou événement particulier**, l'employeur ne peut en aucun cas ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition, **sauf en présence du salarié ou celui-ci dûment appelé**.

L'extrait

« attendu (...) qu'en statuant comme elle l'a fait, alors que l'ouverture des fichiers personnels, effectuée hors la présence de l'intéressé n'était justifiée par aucun risque ou événement particulier, la Cour d'appel a violé les textes susvisés »

(1) Cass. soc. 17 mai 2005.

Isabelle Tellier
isabelle-tellier@alain-bensoussan.com
Sonia Hadjali
sonia-hadjali@alain-bensoussan.com

Indemnisation des préjudices

Conséquences de la location d'une solution informatique défectueuse

▸ Dans le courant de l'année 2000, une agence immobilière a conclu des **contrats de location de matériel informatique** avec la société Espace Infocom, qui a procédé à l'installation matérielle et logicielle du système.

▸ La solution rencontre de multiples **dysfonctionnements** que ni le loueur de matériel, ni la société chargée d'assurer sa maintenance, ne parviennent à résoudre. Le client décide de cesser d'honorer ses loyers et saisit le tribunal de commerce en réparation d'un préjudice estimé à 129 959 €

▸ Le tribunal a condamné Espace Infocom à payer à son client la somme de **63 800 euros TTC à titre de dommages et intérêts** ⁽¹⁾.

▸ Le loueur du matériel ayant saisi la Cour d'appel d'Amiens de cette décision, l'agent immobilier porte sa demande de réparation à la somme de **705 881 euros**. Selon la Cour, cette demande porte sur les **investissements et les dépenses engagés** par un site ayant dû être fermé suite aux difficultés (28 159 € et 11 048 €), une **perte de chiffre d'affaires** (567 083 €), un **trouble commercial et une perte d'image** (50 000 €) et les **coûts de renouvellement du matériel** (22 326 €). Le montant total de ces demandes ne correspond pourtant pas au total indiqué par la Cour (678 615 € seulement, soit une différence de 27 265 €).

Une réparation très faible pour les dommages retenus

▸ La Cour retient la **faute contractuelle** du loueur du matériel qui n'a pas remis à son locataire un bien en état normal de fonctionnement ⁽²⁾.

▸ Pour apprécier les demandes de l'agent immobilier, elle souligne que les dysfonctionnements sont à l'origine de **pertes de temps et d'efficacité** ayant **nuit à son image et d'un manque à gagner**. Elle considère que le **renouvellement du matériel** est justifié mais estime non démontré le lien de causalité entre la fermeture du site et les dysfonctionnements.

▸ Dès lors, il semble que la Cour retienne l'existence des dommages suivants : **perte de chiffre d'affaires, perte d'image et coûts du nouveau matériel**, pour lesquels l'agent immobilier demande une somme totale de **630 409 €**. Cependant, sans fournir plus de précision sur son évaluation des dommages, la Cour estime à seulement **30 000 €** le montant total de l'indemnisation accordée.

▸ La victime des dommages obtient donc une indemnisation très inférieure à celle obtenue en première instance, et qui correspond seulement à **5% des dommages dont l'existence semble retenue**. Les motivations ayant conduit la Cour à retenir ce montant sont inconnues, de même que le sort réservé à la somme de 27 265 € qui ne se retrouve pas dans le détail des dommages invoqués rapporté par la décision.

L'enjeu

La démonstration de l'existence des dommages invoqués ne suffit pas à obtenir leur réparation.

La décision a sans doute considéré que le manque à gagner ayant pour origine les dysfonctionnements était en réalité minime, voire inexistant

(1) TC Compiègne, 15 novembre 2002.

(2) CA Amiens 27 juillet 2004 Espace Info-Com / Avenir Patrimoine

Les conseils

La démonstration de l'étendue des dommages repose autant sur une évaluation justifiée que sur la preuve de la causalité.

Bertrand Thoré
bertrand-thore@alain-bensoussan.com

Fiscalité

La fiscalité du commerce en ligne

Le Modèle de convention fiscale de l'OCDE clarifié

▸ Internet n'est plus seulement un moyen de communication inter-réseaux mais devient un **support d'activités marchandes** conduisant ainsi l'OCDE (Organisation de coopération et de développement économiques) à mettre en place un **cadre fiscal adapté**⁽¹⁾.

▸ Devant le risque de voir assimiler à des redevances de l'article 12 de la convention modèle OCDE, les paiements effectués dans le cadre du commerce électronique, en contrepartie de la mise à disposition ou de l'**utilisation de services en ligne** ou de la **délivrance de produits numérisés**, le groupe technique consultatif (GTC) mis en place a été chargé d'apporter les **clarifications nécessaires** à la classification de ces paiements.

▸ Cette clarification est apparue d'autant plus nécessaire que la délivrance de produits ou services dans le commerce traditionnel ne donne généralement pas lieu à des **paiements qualifiés de redevances**.

Une classification en fonction de la nature de chacune des transactions

▸ Le GTC a **déterminé la qualification** à retenir parmi une **grande variété** de qualification possible (vente de biens meubles, prestation de services, cession ou concession de droit d'auteur, d'équipement scientifique, de savoir-faire ...).

▸ Selon la qualification donnée aux transactions, le **traitement fiscal** des paiements correspondants sera différent : redevances, bénéfices commerciaux ou rémunération d'une prestation de services.

▸ L'élément essentiel à prendre en compte pour la qualification des revenus est la **cause principale du paiement**. si le motif essentiel du paiement est autre chose que l'utilisation ou le droit d'utiliser les droits de propriété intellectuelle ou industrielle, il n'y a pas lieu de prendre en compte l'utilisation incidente de ces droits pour la qualification du revenu correspondant.

Le traitement fiscal des transactions

▸ Les transactions qui confèrent à un acheteur (particulier ou entreprise) le **droit de télécharger**, de stocker et d'utiliser des produits numériques (logiciels, images, sons, textes ...) pour ses propres besoins, ne donnent pas lieu au paiement de redevances, mais d'un **revenu commercial**, dès lors que la cause essentielle du paiement est l'acquisition du produit ou service.

▸ En revanche, les transactions qui ont pour objet principal de transférer à l'une des parties le **droit d'utiliser un droit de propriété intellectuelle** ou industrielle donneront lieu au paiement de **redevances**. Tel sera le cas par exemple, d'un éditeur qui acquiert le droit de reproduire une image protégée par un droit d'auteur et la reçoit par téléchargement.

L'enjeu

Préciser le régime accordé dans les conventions fiscales à différents types de paiements de commerce électronique.

(1) <http://www.oecd.org/>

La règle

L'élément essentiel à prendre en compte pour la qualification des revenus est la cause principale du paiement et non le mode de réalisation de l'opération (par voie électronique ou traditionnel).

Pierre-Yves Fagot
pierre-yves-fagot@alain-bensoussan.com

Actualité

Les sources

Toilettage du Code des postes et des communications électroniques

▸ Afin de tenir compte de la loi du 9 juillet 2004 (dite « Paquet télécom »), le premier ministre opère une **mise à jour** de la **partie réglementaire du Code** des postes et des communications électroniques (CPCE) par décret n°2005-399 du 27 avril 2005⁽¹⁾. Sont notamment concernés, l'organisation et le fonctionnement des **commissions consultatives** (CPCE art. D.99-4 à D.99-5-1), la désignation des membres de la Commission supérieure du service public des postes et des communications électroniques (**CSSPCE**) (CPCE art. D. 96-3) et leurs attributions (CPCE art. D. 96-7 à D. 96-16).

(1) Décret n°2005-399 du 27 avril 2005, JO du 30/04/2005 et rectific. JO du 14/05/2005.

L'ART devient l'ARCEP et élargie ses compétences

▸ L'Autorité de régulation des télécommunications devient l'Autorité de régulation des communications électroniques et des postes (**Arcep**) et régle désormais les **communications électroniques** et les **postes**⁽²⁾.

▸ Le statut de la Poste, le mécanisme de régulation du secteur et le régime de la **responsabilité des prestataires de services postaux** sont réformés. Ainsi, leur responsabilité peut être engagée dans les conditions prévues par les articles 1134 et suivants et 1382 et suivants du Code civil.

(2) Loi n° 2005-516 du 20 mai 2005, JO du 21/05/2005.

Coup d'arrêt à la propagande raciste, antisémite et xénophobe sur internet

▸ La loi contenant le **protocole additionnel** relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques a été adoptée le 19 mai 2005⁽³⁾.

▸ En ajoutant le **racisme** aux **délits** qui peuvent être commis par voie électronique, le protocole additionnel complète ainsi la **Convention européenne** sur la **cybercriminalité** du 8 novembre 2001, premier traité international sur les infractions pénales commises via internet.

(3) Loi n° 2005-493 du 19 mai 2005, JO du 20/05/2005

Vocabulaire des télécommunications / Internet

▸ Deux nouveaux avis de la Commission générale de **terminologie** et de néologie sont parus sur le vocabulaire des télécommunications⁽⁴⁾ et de l'internet⁽⁵⁾. Sont notamment **traduits** et **définis**, les termes suivants : « accès sans fil à l'internet » (ASFI) (équivalent étranger de *wireless Internet access*), « message multimédia » (MMS), « zone d'accès sans fil » (équivalent étranger de *hot spot*), « bloc-notes » (équivalent étranger de *blog*, *web log*, *weblog*), « canular » (équivalent étranger de *hoax*), « modérateur, -trice ».

(4) Cf. JO du 5 mai 2005

(5) Cf. JO du 20 mai 2005.

Directeur de la publication : Bensoussan Alain
 Rédigée par les avocats et juristes de ALAIN BENSOUSSAN SELAS
 Animée par Isabelle Pottier, avocat
 Diffusée uniquement par voie électronique
 ISSN 1634-071X
 Abonnement à : avocats@alain-bensoussan.com

Interview

Un bilan plutôt positif mais avec encore des incertitudes ...

Stéphane Marcovitch, Délégué Général de l'Association des Fournisseurs d'Accès^(*),
par Isabelle Pottier



En quoi consiste exactement l'activité de votre association ?

L'AFA regroupe depuis 1997 les fournisseurs d'accès et les fournisseurs de services Internet avec une double objectif : représenter l'ensemble de la profession des intermédiaires techniques vis-à-vis des pouvoirs publics et fixer des règles déontologiques (pratiques et usages, chartes...). A côté de ces activités, l'AFA gère également le site pointdecontact.net, à la fois site d'information du grand public sur tout sujet pouvant l'intéresser (contenus illicites, spam, protection de l'enfance...) et formulaire permettant aux internautes de signaler des contenus pédopornographiques ou incitant à la haine raciale auxquels ils ont pu être confrontés sur Internet (web, forum, chat...). L'AFA est en contact avec les services de police et de gendarmerie pour leur notifier de tels contenus surtout lorsqu'ils sont hébergés en France, afin d'engager les poursuites nécessaires. Si le contenu est hébergé à l'étranger, l'AFA informe alors la hotline partenaire dans le pays concerné grâce au réseau «Inhope» regroupant des hotlines partenaires dans les pays de l'Union européenne, mais aussi aux Etats-Unis, Corée, Australie, Taiwan... Le réseau permet de traiter le problème au niveau local très rapidement sans avoir à mettre en oeuvre la coopération judiciaire internationale.

La LCEN a-t-elle révolutionné les pratiques de vos adhérents ? les échos sont-ils positifs ?

Rappelons que la LCEN est d'abord la transposition de la directive communautaire sur le commerce électronique. Ce texte était très attendu car il était nécessaire de clarifier le régime de responsabilité des intermédiaires techniques. Il a donné lieu à beaucoup de débats notamment sur le projet d'obliger les fournisseurs d'accès (FAI) et hébergeurs à surveiller les contenus illicites. Notre mobilisation a été payante puisque cette obligation s'est muée en une obligation de signalement qui, dans la déontologie de l'AFA, existait déjà et a donc été généralisée à l'ensemble des FAI et hébergeurs. La solution est moyennement satisfaisante en ce qui concerne la coupure par les hébergeurs une fois qu'ils ont connaissance d'un contenu illicite. Notre souhait était une coupure sur décision de justice car, hormis les cas flagrants, le FAI n'est pas toujours à même de décider si le contenu qu'on lui soumet est licite ou non, notamment en matière de contrefaçon et de diffamation. Même si l'option retenue par le législateur ne concerne finalement que les contenus «manifestement» illicites, il risque d'y avoir des cas dans lesquels la responsabilité des hébergeurs sera engagée ... tout dépendra de l'interprétation des juges (1). Le bilan est plutôt positif mais avec encore des incertitudes sur la mise en oeuvre de cette loi.

Quelles sont selon vous, les questions que la loi n'a pas encore résolues ?

Celles relatives aux poursuites pénales des spammeurs. L'AFA souhaitait qu'à l'occasion de ce texte, les prestataires de messageries (fournisseurs d'accès ou de webmail) aient la possibilité d'engager de telles poursuites dissuasives. Or, ils ne le peuvent qu'en ayant recours à la loi Godfrain sur la fraude informatique dans le cas très exceptionnel où le spam aurait été tellement massif qu'il aurait paralysé le serveur. On sait que les particuliers portent rarement plainte, c'est pourquoi, nous souhaitons que les prestataires de services puissent bénéficier des mêmes droits que les parties civiles et forcer ainsi le déclenchement de l'action publique. Nous allons néanmoins continuer d'œuvrer pour l'obtenir...

(*) <http://www.afa-france.com/>

(1) TGI Paris, 17ème ch, 15/11/2004, <http://www.foruminternet.org/telechargement/documents/tgi-par20041115.pdf>