Caprioli & Associés

Technologies, Information et Propriétés Intellectuelles

TiPi n° 10
Printemps 2011

L'édito de la TiPi :

Prospective 2011-2015 : un nouveau cycle de Directives européenne pour l'économie numérique : du pain sur le clavier en perspective pour les Etats membres et les acteurs économiques.

De nombreux changements législatifs s'annoncent pour les années à venir en matière de droit de l'économie numérique ! Pourtant, les deux directives du 25 novembre 2009 (2009/136/CE et 2009/140/CE publiées au JOUE du 18 décembre 2009) avaient donné le ton sur les obligations de notification des failles de sécurité et en matière de données personnelles. Leur transposition en France doit intervenir au cours du printemps.

Le début de l'année 2011 a commencé très fort avec deux consultations de la Commission européenne dans le but de procéder à la révision de la directive 95/46 du 24 octobre 1995 sur la protection des données à caractère personnel et de la directive sur les signatures électroniques du 13 décembre 1999.

Des adaptations de ces textes sont nécessaires en raison des évolutions technologiques et des pratiques commerciales. Mais les motivations sont différentes dans les deux hypothèses de travail.

Dans le cadre de la protection des données personnelles, la directive pose des obligations et l'idée sous-jacente est plutôt de modifier le texte afin de mieux encadrer les nouvelles pratiques telles que notamment la biométrie, la lutte contre les fraudes dans le numérique, la géolocalisation, les moteurs de recherche, les réseaux sociaux, ou encore le respect du droit à l'oubli. Au contraire, dans la seconde directive, la question posée consiste à se demander pourquoi, les signatures électroniques ne sont que peu déployées dans les Etats membres ? De plus, en s'inscrivant dans la perspective tracée lors du colloque des Nations Unies (CNUDCI) sur le commerce électronique des 14-16 février 2011, la Commission s'interroge sur les très importantes questions juridique et technique de l'authentification et de l'identification : faut-il légiférer sur ces aspects ? De même est-ce que les personnes morales pourront manifester leur consentement en signant des documents et des contrats ? etc.

S'agissant par ailleurs de la Directive sur le commerce électronique du 8 juin 2000, on ne voit pas comment elle peut rester en l'état dans la mesure où elle a été élaborée à la fin des années 90, avant l'avènement du Web 2.0, et des nouveaux modèles commerciaux tels que Google, Facebook, E-bay et autres YouTube. D'ailleurs, la jurisprudence de la Cour de cassation française ne coïncide pas toujours avec celle des autres Etats membres sur de nombreux points (ex : les sites parking de noms de domaine).

En outre, ne faut-il pas (déjà !) modifier la directive sur les droits d'auteur et les droits voisins dans la société de l'information (22 mai 2001) dès lors que la protection des droits sur l'internet n'est toujours pas réglée notamment en France avec les lois Hadopi I, II, et bientôt III.

Bref, on l'a compris les données de l'environnement changent avec les nouvelles pratiques du web, et le cadre juridique doit être adapté ! Les entreprises avisées ne manqueront pas d'assurer une veille juridique « active » sur l'ensemble de ces sujets qui sont susceptibles d'affecter leurs métiers et leur fonctionnement, et donc leur chiffre d'affaire !

Eric A. CAPRIOLI
Avocat à la Cour de Paris
Expert aux Nations Unies

Aujourd'hui dans la TiPi :

Actualités :

La simplification de certaines démarches administratives

Le décret n° 2011-167 permet, à compter du 1er mars 2011, aux organismes légalement fondés à requérir des actes de l'Etat civil (administrations, services et établissements publics de l'Etat ou des collectivités territoriales, les caisses et organismes gérant des régimes de protection sociale et les notaires), de demander directement auprès des officiers de l'Etat civil dépositaires de ces actes, la vérification des données fournies par les usagers. Le décret, qui introduit un titre III au sein du décret n° 62-921 du 3 août 1962 modifiant certaines règles relatives aux actes de l'Etat civil (articles 13-2 à 13-5 nouveaux), prévoit que les usagers soient préalablement informés de la demande de vérification.

Ainsi, conformément au nouvel article 13-4, l'officier d'Etat civil saisi est tenu de vérifier la conformité des informations reçues à celles figurant sur l'acte d'état civil, qu'il peut compléter ou rectifier dans la limite de la demande qui lui a été adressée. Lorsque la demande est effectuée par voie électronique, elle doit l'être dans des conditions qui garantissent l'intégrité, la sécurité et la confidentialité de la transmission, l'identité et la fonction de l'expéditeur et celles du destinataire.

Décret n° 2011-167 du 10 février 2011 instituant une procédure de vérification sécurisée des données à caractère personnel contenues dans les actes de l'Etat civil, J.O. du 12 février 2011, p. 2739.

Nouvelle mission pour l'ANSSI

Le décret n° 2011-170 du 11 février 2011 modifiant le décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » confie une mission supplémentaire à l'ANSSI.

Conformément à l'article 1, l'ANSSI assure « *la fonction d'autorité nationale de défense des systèmes d'information. En cette qualité et dans le cadre des orientations fixées par le Premier ministre, elle décide les mesures que l'Etat met en œuvre pour répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale et elle coordonne l'action gouvernementale* ».

Ce renforcement des missions de l'ANSSI s'inscrit dans la stratégie de la France en matière de défense et de sécurité des systèmes d'information.

Décret n° 2011-170 du 11 février 2011 modifiant le décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », J.O. du 13 février 2011.

Avènement de la lettre recommandée électronique

Le décret n° 2011-144, pris en application de l'article 1369-8 du code civil, vient préciser les caractéristiques de la lettre recommandée envoyée par voie électronique en reprenant les principales dispositions relatives au dépôt et à la distribution de ces envois qui peuvent être soit tout électroniques, soit hybrides (réception du courrier papier).

L'article 1er vient ainsi indiquer les informations obligatoires que le tiers en charge de l'acheminement doit communiquer préalablement à l'envoi d'une lettre recommandée électronique, ainsi que celles que l'expéditeur doit indiquer lors du dépôt d'une LRE.

L'article 2 énonce les modalités propres à la preuve de dépôt renvoyée par le tiers en charge de l'acheminement à l'expéditeur (éléments constitutifs, délai de conservation, accessibilité). L'article 3 prévoit les modalités d'acceptation de la LRE ainsi que les conditions entourant l'avis de réception.

Les articles 4 et 5 ont trait à la distribution et à la remise des lettres recommandées hybrides par le biais de prestataires de services postaux.
On attend toujours le décret relatif à la présomption (simple) de fiabilité de la datation électronique des envois et des réceptions.

Décret n° 2011-144 du 2 février 2011 relatif à l'envoi d'une lettre recommandée par courrier électronique pour la conclusion ou l'exécution d'un contrat, J.O. du 4 février 2011 p.2274. Pour un commentaire, v. Eric A. Caprioli, Communication Commerce électronique, avril 2011, p. 44 et s.

DSI : L'Etat aussi

Le décret n° 2011-193 du 21 février 2011 crée une direction interministérielle des systèmes d'information et de communication de l'Etat, dont les missions sont les suivantes : orienter, animer et coordonner les actions des administrations de l'Etat visant à améliorer la qualité, l'efficacité, l'efficience et la fiabilité du service rendu par les systèmes d'information et de communication ; veiller à ce que ces systèmes concourent de manière cohérente à simplifier les relations entre les usagers et les administrations de l'Etat et entre celles-ci et les autres autorités administratives au sens de l'ordonnance du 8 décembre 2005 ; organiser et piloter la conception et la mise en œuvre des opérations de mutualisation entre administrations de l'Etat, ou entre celles-ci et d'autres autorités administratives, de systèmes d'information ou de communication d'usage partagé ; contribuer, par les réponses apportées aux besoins propres de l'Etat en matière de technologies de l'information et de la communication, à promouvoir l'innovation et la compétitivité dans ce secteur de l'économie nationale.

Décret n° 2011-193 du 21 février 2011 portant création d'une direction interministérielle des systèmes d'information et de communication de l'Etat, J.O. du 22 février 2011.

Publication de la LOPPSI II

La loi d'orientation et de programmation pour la performance de la sécurité intérieure (improprement appelée LOPPSI II) vient d'être publiée au Journal Officiel après de multiples péripéties législatives, notamment une censure de 13 articles par le Conseil constitutionnel : Décision du Conseil constitutionnel n° 2011-625 DC du 10 mars 2011 (partiellement conforme).

Rappelons que cette loi « fourre tout » comprend des dispositions nouvelles visant à lutter contre la cybercriminalité comme la création d'un nouveau délit d'usurpation d'identité applicable également sur les réseaux de communication au public en ligne. Elle aggrave les sanctions de certains délits de contrefaçon et accroît la protection des internautes contre les images de pornographie enfantine. Elle adapte, ensuite, les moyens d'enquête aux nouvelles technologies afin d'améliorer les procédures d'investigation techniques et scientifiques et simplifie les procédures d'alimentation du fichier national automatisé des empreintes génétiques. Elle améliore, également, les procédures d'enregistrement et de contrôle des délinquants sexuels et aménage le régime juridique de la vidéo protection.

La loi améliore, enfin, la protection des intérêts fondamentaux de la Nation, renforce la répression des infractions commises dans des enceintes sportives et renforce la lutte contre l'insécurité routière. Elle modifie par ailleurs les compétences du préfet de police de Paris.

Nous reviendrons sur cette loi dans un prochain numéro de la TiPi.

Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, J.O. du 15 mars 2011 p. 4582.

Publication du décret d'application de l'article 6 de la LCEN

Attendu depuis près de 7 ans, le décret n° 2011-219 du 25 février 2011 vient préciser les données d'identification des abonnés des fournisseurs d'accès et d'hébergement qui doivent être conservées vertu de l'article 6 II et II bis de la Loi pour la Confiance dans l'économie numérique du 21 juin 2004 (LCEN), cette conservation étant le corollaire du régime de responsabilité limitée dont ils bénéficient quant aux contenus mis en ligne. La conservation, d'une durée de 1 an, vise une large catégorie de données relatives aux connexions des abonnés, aux opérations de connexion, aux informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte mais aussi pour les informations relatives au paiement (art. 1).

En outre, le décret prévoit un chapitre II relatif aux demandes administratives prévues à l'article II bis de la LCEN (actes de terrorisme) en énonçant les modalités propres aux demandes formulées par les agents.

Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, J.O. du 1er mars 2011, p. 3643.

Focus :

Les risques juridiques du Cloud Computing - Là haut dans les Nuages

Le Cloud computing, l'Informatique en Nuages… Quelle poésie dans le nom donné pour cette forme « nouvelle » d'externalisation informatique ! Il s'agit de l'utilisation de serveurs informatiques répartis dans le monde entier et liés à un réseau (comme l'internet) (1). Les utilisateurs ne sont plus propriétaires **que** des données qui y sont hébergées et non des applications ou de l'architecture qui permet leur utilisation ou leur hébergement.

Les nuages renvoient immanquablement à un sentiment de liberté, d'évasion, c'est sans doute pourquoi Google a recouru à cette image en août 2006 lorsqu'il a présenté ce nouveau modèle d'architecture technique (2)... Oui, mais un nuage est sans forme et surtout, il peut être synonyme d'orages, voire de pluies toxiques. Ainsi, une application phare du Cloud computing, Gmail, le service de courrier électronique de Google, a été en panne par deux fois ces dernières années. La première panne remonte au mois de février 2009, suivie d'une autre en mai où plusieurs services phares (Google Search, Google News, Google Docs, Google Talk, Picasaweb) de Google ont été fortement perturbés.

Les nuages noirs s'amoncellent progressivement sur ce que l'on peut considérer comme une approche marketing d'externalisation informatique. Il est vrai que l'avantage majeur du Cloud computing consiste pour les utilisateurs à pouvoir accéder de manière évolutive à de nombreux services en ligne (service de stockage de données, de traitement de texte, voire des applications de sécurité…) sans avoir à gérer l'infrastructure informatique, ce qui induit bien évidemment des économies budgétaires conséquentes. Cette solution semble donc idéale en cette période de rigueur pour les entreprises.

D'autant que l'engouement au profit du Nuage provient en général des services opérationnels, souscrivant parfois directement les services du Nuage en contournant à cette occasion DSI, RSSI, Direction des achats, Direction juridique ou encore Direction de la conformité.

Oui, mais voilà : la solution idéale n'existe pas et le Cloud computing qui ne serait pas parfaitement encadré juridiquement fait peser de nombreux risques juridiques, ayant trait notamment à la disponibilité (I), à la conformité légale (II), à la confidentialité (III) ou encore à la sécurité des données confiées au Nuage (IV). Au caractère évanescent, poétique du Nuage, le juriste rappelle les bénéfices immédiats d'une approche juridique ciselée pour faire appel à ce Nuage en toute sérénité/sécurité comme dirait Baudelaire « *pour que le ciel ne soit pas bas et lourd* ».

(1) Selon le CIGREF, « *Le cloud computing permet de consommer et d'acheter des services IT Dans le monde à travers un réseau. Il s'articule autour de quatre critères clés :*

- *La mutualisation des ressources ;*
- *Le paiement à l'usage ;*
- *La modularité ;*
- *La standardisation des fonctions proposées* ».

(CIGREF, Impact du Cloud computing sur la fonction SI et son écosystème, octobre 2010, disponible sur le site www.cigref.fr). Cette définition est à rapprocher de celle fournie par l'ENISA (p. 14) in *Benefits, risks and recommendations for information security*, novembre 2009, www.enisa.europa.eu.

(2) D. Guinier, *L'informatique dématérialisée en nuages - Ontologie et sécurité du Cloud Computing* ; Expertises 2010 ; n° 351 ; p 335 et s.

I. La disponibilité des données

Le client doit avant tout déterminer le **périmètre des données** qu'il souhaite confier à un prestataire, afin que celui-ci puisse avoir la possibilité de préserver les données les plus sensibles en interne, de sorte qu'elles soient toujours disponibles.

Le client doit également pouvoir y accéder rapidement en cas de demande formulée par un administrateur technique ou un salarié habilités à cette fin. A ce titre, la **gestion des droits d'accès** constitue un élément important qu'aucun client ne doit (ni ne peut) négliger.

Dans cette hypothèse, le prestataire doit s'engager sur la qualité et les performances de son « Nuage », le plus souvent par le biais d'une **convention de niveaux de services (Service Level Agreement ou SLA).** Elle permet de veiller au respect, par le prestataire et ses éventuels sous-traitants, des niveaux de services associés aux architectures techniques ainsi qu'aux solutions applicatives. Il s'agira de déterminer les indicateurs (souvent évolutifs) eu égard aux résultats escomptés par le client. **Une clause de pénalité – point souvent difficile**

lors des négociations – viendra sanctionner tout manquement à ces indicateurs (3). Le SLA peut également inclure d'autres référentiels de qualité et de sécurité liés à l'externalisation du ou des systèmes d'information (mise en place de **tests et jeux d'essais, clause de recette, audits internes ou externes, politique de sécurité**).

(3) Voir *La QoS, un concept central pour la gestion de la sécurité des SI*, Pascal Agosti, décembre 2008, http://www.globalsecuritymag.fr/Pascal-Agosti-Cabinet-Caprioli,20081223,6729.html

Cette disponibilité n'est pas seulement exigible lorsque les relations avec le prestataire du Nuage sont au beau fixe, mais également :

- si le prestataire met la clé sous la porte de façon brusque (tous les prestataires n'ont pas l'assise financière de Google) ;
- si le prestataire décide d'arrêter cette activité à très court terme (d'où l'importance des clauses *ad hoc* dans le contrat assurant une certaine pérennité) ;
- s'il est racheté par un concurrent et que le client ne souhaite pas continuer avec ce dernier (tous les clients ne veulent pas forcément traiter avec Google) ;
- si la prestation proposée ne correspond pas au niveau de qualité attendue ;
- ou encore si des fautes ont été commises par le prestataire.

Bref, les conditions pour mettre un terme à la relation contractuelle avec le prestataire sont nombreuses et le client ne doit pas se trouver pieds et poings liés avec ce dernier, au risque de voir ses services bloqués parfois pendant de longs mois. **La clause de réversibilité** constitue à cet effet une solution pertinente.

Cette clause **devra préciser l'ensemble des modalités pratiques de fonctionnement du système d'information pendant la durée de la phase de réversibilité.** Il s'agira de définir les garanties apportées par le prestataire pour assurer la continuité du service sans remise en cause des niveaux de services attendus. Il est évident que les données hébergées sur le système d'information devront faire l'objet d'un soin particulier. Tous ces éléments figureront dans le **plan de réversibilité** que les parties auront pris soin de négocier au moment de la signature du contrat d'externalisation. Au vu du caractère planétaire, disparate et « opaque » de certains Nuages, il est à noter ici que les parties ne pourront faire **l'économie d'identifier tous les serveurs utilisés pour héberger les données du client**, la **traçabilité** de chaque donnée du client restant un élément essentiel de sécurité tant technique que juridique (sur quel serveur est la donnée ? Qui peut y accéder ? Selon quels droits ?), comme rappelé ci-après.

II. La conformité légale

Rappelons qu'en cas de non respect des règles impératives encadrant les données stockées dans le Nuage, le client pourra être reconnu responsable non seulement vis-à-vis de son droit local mais, le cas échant, vis-à-vis de la législation du lieu où se situe le serveur informatique. De plus, certains secteurs ou certains type de données nécessitent des mesures particulières (par exemple, le secteur bancaire est soumis à une réglementation très exigeante en matière de contrôle interne, le Règlement CRBF 97-02, les factures électroniques sont soumises à des règles strictes de conservation, etc.) en cas d'externalisation de données, qui imposent notamment une exigence de visibilité parfaite du lieu de stockage réel des données.

Le cas le plus symptomatique de cette réalité est celui de l'hébergement de données du client dans le Nuage, à sa demande et alors que ce sont des données à caractère personnel, qui peuvent être, par exemple, relatives à ses salariés, à ses clients ou prospects, ainsi qu'à ses fournisseurs. Or, le responsable du traitement – à savoir le client – doit, conformément à l'article 34 de la loi Informatique et Libertés, « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.* ». Lorsqu'il délègue la gestion des traitements au prestataire, le client doit s'assurer que celui-ci dispose des « *garanties suffisantes* » en matière des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer. Une « *garantie suffisante* » pourrait être de s'assurer de la situation financière de son prestataire. Surtout, la délégation de la gestion ne signifie en rien la délégation de la responsabilité : le client reste responsable, y compris pénalement du respect des obligations

légales par le prestataire, conformément à l'article 35 de la loi Informatique et Libertés.
Cet article prévoit également que le contrat d'externalisation entre le client et son prestataire devra être passé par écrit et comporter les obligations du prestataire en terme de protection de la sécurité et de la confidentialité des données à caractère personnel et des mesures techniques y afférentes.

Le client devra donc faire attention au choix de son prestataire. En effet, ce dernier aura intérêt à être installé dans un pays qui dispose de règles de droit en matière de protection des données à caractère personnel au moins aussi protectrices que celles en vigueur dans l'Union européenne. Si la protection des données n'est pas suffisamment assurée par le pays du prestataire, le transfert n'est pas possible, sauf à ce que le prestataire fournisse des garanties suffisantes en matière de sécurité.

En outre, les données à caractère personnel qui seraient traitées hors de l'Union européenne ou d'un pays à régime de protection « adéquat » imposent nécessairement le respect de formalités CNIL particulières (clauses spécifiques, autorisation de la CNIL, etc.)

III. La confidentialité

Par définition, de multiples données issues de clients différents peuvent partager le même Nuage. Il faut donc s'assurer de leur confidentialité et de l'étanchéité des données, notamment en application des réglementations mentionnées ci-dessus.

Le prestataire doit donc prendre les **mesures adéquates pour assurer le chiffrement des données d'un client, leur isolement technique mais aussi le choix des personnels (superviseurs, administrateurs…) qui pourraient accéder aux données**. Les conditions d'embauche peuvent constituer un facteur important de sécurité : l'élément humain ne doit pas être négligé car il constitue fréquemment une faille dans les organisations les mieux huilées.

Une clause de confidentialité doit être détaillée dans son champ d'application matériel (personnes qui doivent respecter cette obligation, contenu de l'obligation), temporel et devrait être complétée d'une **clause pénale (ou clause de dommages-intérêts en faveur du client)**, sanctionnant en sus tout manquement constaté par le prestataire ou son personnel.

IV. La sécurité des données

Toutes les mesures décrites ci-dessus concourent à la sécurité des données externalisées par le client. Toutefois, il appartient aux entreprises de reprendre la main sur la problématique du Nuage et d'exiger des prestataires, avant de leur confier les données de l'entreprise, le **respect de certaines normes techniques telles que les normes ISO/CEI 27001 et ISO 27005, fixant les méthodes et pratiques en matière de système de management de la sécurité de l'information (SMSI).**

En outre, certaines briques de Cloud Computing peuvent reposer sur des **modules de logiciels libres** (ex : Open Cloud Consortium créé au printemps 2008). Il appartient donc aux entreprises d'identifier les effets juridiques des licences de tels modules (Quelle licence est utilisée ? Est-elle contaminante pour le SI interne de l'entreprise ?...) et de déterminer les conséquences de cette utilisation pour la sécurité juridique de l'entreprise. Le prestataire doit également être autorisé à effectuer des audits et des **tests d'intrusion sur les serveurs du prestataire pour s'assurer du niveau de sécurité global de ce dernier.**

Un client doit avoir confiance dans le prestataire à qui il va confier ses données. Au plan juridique, le Nuage se doit d'être transparent.

Un Nuage qui pourrait faire le beau temps ;

Que c'est charmant !

Signaux de fumée (en direct du web…)

La Cour de cassation a finalement décidé le 17 février 2011 que la commercialisation d'espace publicitaire sur le site ne faisait pas perdre le statut d'hébergeur, contrairement à ses affirmations précédentes (arrêt « Tiscali » du 14 janvier 2010) : le régime de responsabilité atténuée des hébergeurs posée par la LCEN du 21 juin 2004 s'applique donc aux sites web 2.0, et pas seulement aux services ne proposant qu'un service purement technique de stockage informatique des contenus.
Arrêt de la 1e chambre civile de la Cour de cassation - n° 165 du 17 février 2011 (09-67.896)

Pour la présidente de la Commission de protection des droits de la HADOPI qui s'est exprimée sur le sujet en février, l'adresse IP n'est pas une donnée à caractère personnel (« *c'est la jurisprudence de la Cour de cassation* »). Si l'on comprend la raison d'une telle affirmation (faciliter les poursuites de la Commission de protection chargée de sanctionner les internautes au sens de la réglementation HADOPI), **la problématique semble plus complexe (voir notre analyse dans notre TiPi n°7).**
http://www.numerama.com/magazine/18084-l-hadopi-affirme-que-l-adresse-ip-n-est-pas-une-donnee-personnelle.html

Jurisprudences :

Quand l'annonceur est engagé par le contenu de ses publicités…

Un document publicitaire peut-il engager la responsabilité de son auteur ? L'arrêt de la première chambre civile de la Cour de cassation du 6 mai 2010l'admet sans équivoque.

En l'espèce, une mère, séduite par la brochure publicitaire d'une société commerciale spécialisée dans la formation professionnelle, décide se souscrire un contrat au profit de son fils.

Apparait sur toutes les brochures publicitaires, ainsi que sur le site internet, que la société en question s'engage fermement à trouver un employeur aux jeunes gens intéressés par leurs cours. Rien n'ayant été proposé dans ce sens à son fils à l'issue de la formation, la défenderesse estime que la société n'a pas respecté ses engagements, et refuse de régler les frais de scolarité. **Or l'engagement en question, qui figure dans les documents publicitaires de la société, n'a été repris ni dans le contrat, ni dans les conditions générales de vente.**

C'est d'après ce postulat qu'en première instance, les juges n'ont pas retenu le manquement de la société à son obligation contractuelle. Cette solution aurait pu convaincre, en effet, se fondant sur le fait que les engagements contenus dans les publicités ne s'appuient par principe sur aucune volonté ferme de contracter. Il est fréquent que l'annonceur exclut expressément leur propre valeur contractuelle et y insère une mention « document non-contractuel ».

Pourtant la Cour de cassation censure la décision des juges du fond considérant que ***« les documents publicitaires peuvent avoir une valeur contractuelle dès lors que, suffisamment précis et détaillés, ils peuvent avoir une influence sur le consentement du cocontractant ».*** Pour la Cour, c'est donc sans rechercher si la publicité était suffisamment claire et précise pour déterminer le consentement de la cliente que le tribunal s'était prononcé.

Dans cette affaire, la Cour de cassation a préféré suivre une logique de cohérence plutôt que de se borner à considérer que la publicité ne pourrait pas, par nature, constituer un document contractuel.
En effet, si l'objectif même de la publicité est d'attirer le client et de déterminer son consentement, il apparaît logique que le professionnel réponde des engagements qu'il prend même dans ses annonces publicitaires, si celles-ci sont suffisamment **fermes, précises et claires** pour que le cocontractant puisse légitimement attendre leur réalisation. **L'annonceur ne pouvant pas nier l'influence certaine que les objectifs visés dans les annonces peuvent avoir sur la détermination du client à souscrire le contrat**. En revanche le fait de fonder l'arrêt au **visa de l'article 1134 du Code Civil** et non de l'article L. 121-1 du Code de la Consommation relatif à la tromperie, révèle la volonté du juge de ne pas se placer dans le rapport consommateur-entreprise, mais plus généralement dans celui d'un contrat, et ceci dans un souci d'indemnisation. Peut-être peut-on malgré tout regretter que la question n'ait pas été tranchée sur le terrain du dol.

Quoi qu'il en soit, cette décision a pour conséquence principale de rappeler que le champ des obligations contractuelles de l'annonceur n'est pas forcément cantonné au seul « contrat ». Il est susceptible de répondre de ses engagements pris dans le cadre de la publicité qu'il formule.
Alors prudence ! En intégrant ainsi la publicité dans la sphère contractuelle, la Cour de cassation invite expressément les professionnels à garder une certaine réserve dans les allégations qu'ils font figurer dans leurs brochures publicitaires. Dès lors que celles-ci sont **« claires »** et **« précises »**, et créent une **attente légitime** du public auquel elles s'adressent, il y a fort à parier que les juges pourraient être enclins à retenir l'inexécution contractuelle là où l'on aurait pu voir une simple publicité « *trompeuse* » ou de nature à induire en erreur.

Signaux de fumée (en direct du web…)

Le TGI de Montpellier a rendu une ordonnance de référé le 20 octobre 2010 appliquant à Google Inc la loi Informatique, Fichiers et Libertés. Il l'a condamné (sous astreinte) à supprimer de ses moteurs de recherche tous les résultats apparaissant à la suite de requêtes associant une institutrice à une ancienne vidéo à caractère pornographique http://legalis.net/spip.php?page=jurisprudence-decision&id_article=3121

Le site http://www.voiture-volee.com, officiellement basé au Panama, proposait depuis plusieurs semaines de mettre en relation des particuliers qui souhaiteraient acheter ou vendre des voitures volées, en toute confidentialité. **La DGCCRF et Interpol ont été saisis… mais il s'agissait d'un plan marketing viral lancé par une entreprise d'enchères inversées en ligne !**

Recel d'informations et espionnage

Contrairement aux idées reçues, **le vol d'informations n'est en aucun cas qualifié pénalement. Pour ce faire, une soustraction frauduleuse est nécessaire !**

Portant le patrimoine informationnel d'une entreprise a une réelle valeur financière et stratégique qu'il convient de protéger de manière efficace. Or peut-on assimiler l'information, élément incorporel, à une « *chose* » tel que l'entend le législateur ?

Sur cette question récurrente, la Cour de Cassation ne semble pas s'être prononcée. Par contre, **dans un arrêt du 20 octobre 2010 (1)**, en procédant à une **interprétation très extensive des dispositions de l'article 321-1 du Code Pénal relatif au recel, elle ouvre la possibilité d'une solution alternative** en cas de détournement de fichiers informatiques « *provenant d'un vol* ».

Dans les faits d'espèce, un salarié licencié de la société de surveillance ADT France a adressé les fichiers clients de cette dernière à une société concurrente. Faute d'élément probant ou par précaution, la Haute juridiction n'a pas retenu la condamnation pour vol mais, **elle a approuvé la Cour d'Appel d'avoir caractérisé le recel des « *fichiers clients* » et « *d'éléments provenant d'un vol* ».**

Pour appliquer cette qualification, le raisonnement a consisté tout d'abord dans le choix du terme **« élément » : expression suffisamment vague pour pouvoir désigner tant le contenant que le contenu**.

Ensuite, pour éviter d'assimiler « l'information » à la « chose » telle qu'énoncée dans l'alinéa premier de l'article 321-1 du Code Pénal, **la haute juridiction fonde sa décision sur le deuxième alinéa de ce même article : le recel-profit, qui lui porte plus largement sur le « produit » de l'infraction** : « *Le recel est le fait de dissimuler, de détenir ou de transmettre **une chose**, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit**. Constitue également un recel le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit* ».

Le recel-profit est alors constitué non par la simple acquisition de l'information, mais par l'exploitation de celle-ci.

Ainsi, apparaît-il que, si le droit pénal français ne protège pas tant l'entreprise contre l'appréhension de l'information (le vol) comme c'est le cas en l'espèce, le juge protège davantage celle-ci contre sa divulgation ou son détournement. Dès lors, deux hypothèses prétoriennes semblent être dégagées : le recel d'information peut être caractérisé, soit au titre du premier alinéa de **l'article 321-1 de Code Pénal** qui suppose **la détention du support**, soit au titre **du deuxième alinéa** lorsque les **renseignements obtenus font l'objet d'une exploitation** par le receleur.

Prudence toutefois car la juridiction ne pose aucun principe et s'est intéressée uniquement aux faits de l'espèce ! Cet arrêt reste donc très clairement à interpréter avec une grande prudence. Il ne saurait que trop être conseillé à la direction d'une entreprise de prendre des mesures techniques et organisationnelles en amont afin d'éviter les « fuites », le manque de sécurité pouvant par ailleurs lui être reproché en fonction des données accédées (données à caractère personnel, données bancaires, etc.).

(1) Cass. crim., 20 octobre 2010, n° 09-88.387, inédit.

Formations - Conférences :

Séminaire Voirin Consultants, « Les réseaux sociaux d'entreprise : un pas vers l'intelligence collective ? » : les enjeux juridiques, E. Caprioli et F. Coupez, 24 mars 2011, Paris (renseignements alexia.marjolet@voirin-consultants.com).

AFNOR, Le Club des adhérents, « Cloud computing : plateformes d'applications et services distribués : enjeux juridiques », E. Caprioli, 25 mars 2011, Paris.

Barreau de Nice, Ecole des avocats – Formation continue, Technologie de l'information et droit du travail : cyberprotection ou cybersurveillance ? E. Caprioli, 25 mars 2011, Paris.

AFCDP, réunion sur le thème « Réseaux Sociaux : Quelles questions un CIL doit-il se poser ? », F. Coupez, 31 mars 2011, Paris.

Comundi, Cybersurveillance des salariés, F. Coupez, 25 et 26 mai 2011, Paris.

Rencontre Evénementielle du Forum des Compétences, Obligations en matière de Sécurité de l'Information, E. Caprioli, 25 mai 2011, Paris.

Une réponse… à une question :

Le cabinet a sélectionné une question concernant la diffamation sur les réseaux : un cas d'e-réputation.

Que faire en cas de propos « diffamants » sur un forum de discussion ?

La diffamation, le dénigrement ainsi que les autres atteintes à l'honneur et à la vie privée s'accommodent facilement de l'internet ; des internautes indélicats pensant bénéficier d'une impunité (toute relative) postent des messages au contenu litigieux, allant de la simple moquerie à la critique la plus sévère, quand leurs propos ne débordent pas sur la diffamation, voire à l'injure ordurière. Les cibles privilégiées de ces excès sont bien souvent les employeurs, les hommes politiques ou d'autres connaissances plus ou moins proches de l'internaute.

Que faire face à ce type de comportement litigieux et préjudiciable ?

En France, outre la voie pénale classique, fondée sur la loi de la presse du 29 juillet 1881, la LCEN a posé un principe de notification des contenus manifestement illicites par les personnes estimant avoir subi un dommage du fait de ces contenus à l'article 6-I-5 : pour l'éditeur du contenu puis, dans un second temps, pour l'hébergeur du contenu. Ainsi, la connaissance des faits litigieux est présumée acquise par l'hébergeur lorsque lui sont notifiés les différents éléments suivants :

- la date de notification ;
- les éléments permettant l'identification du notifiant ;
- les éléments d'identification du destinataire de la notification ;
- la description des faits litigieux et leur location précise ;
- les motifs pour lesquels les contenus doivent être retirés comprenant la mention des dispositions légales et des justifications de fait ;
- la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté.

Reste que la Cour de cassation a eu l'occasion, dans deux arrêts du 17 février 2011 (affaire « Amen » et affaire « Dailymotion »), de préciser que ces informations devaient figurer de façon obligatoire dans la notification pour pouvoir, par la suite, engager leur responsabilité de l'hébergeur.

En effet, si l'hébergeur ou l'éditeur des contenus illicites ne retirent pas les contenus diffamants, une voie judiciaire est ouverte pour obtenir un retrait sous astreinte et la réparation du préjudice (assignation devant le TGI, éventuellement en référé). Notons toutefois qu'il existe des garde-fous visant à encadrer ce dispositif et permettant, notamment en cas de notification abusive, de sanctionner pénalement ces abus.

Lorsque l'auteur ou l'hébergeur sont situés en dehors de France, il conviendra alors de prendre en considération la gageure de l'exécution des décisions judiciaires à l'étranger (exequatur) et de déterminer au cas par cas les voies de recours pertinentes et les règles applicables en la matière.

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

Vie du cabinet :

Le Cabinet souhaite la bienvenue à Aurélie GURFINKIEL, avocat à la Cour de Paris et à Fabienne PITIOT, élève avocate au Barreau de Nice. Nous sommes heureux de les compter dans notre équipe.

Le 28 mars, le Cabinet parisien s'agrandit et déménage au 29 rue Mogador, toujours dans le neuvième arrondissement de Paris.

Les coordonnées téléphoniques ne changent pas.

TiPi dans le détail :

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

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

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

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