

L'IMPACT DES NOUVELLES TECHNOLOGIES SUR LES APPELS D'OFFRES

Les CAO peuvent-elles recourir à la vidéoconférence ?

- Le ministre de l'Economie a récemment répondu à une question d'un parlementaire qui l'interrogeait sur la possibilité de comptabiliser dans le quorum, les membres d'une commission d'appel d'offres (CAO) assistant à la réunion par **vidéoconférence** (1).
- En l'espèce, l'intérêt de cette question réside davantage dans l'interrogation du parlementaire que dans la réponse du ministre, qui se borne à rappeler que comptabiliser au quorum la présence d'un membre de la CAO qui aurait assisté à la réunion par vidéoconférence est impossible de « *lege lata* » (en vertu de la loi).
- Aucun texte n'envisage la possibilité de considérer que les membres qui participent à l'assemblée par visioconférence sont réputés présents pour le calcul de ce quorum. Cette possibilité n'est en conséquence **juridiquement pas admise**.
- Le ministre a néanmoins déclaré qu'il « **étudie** » cette proposition qui nécessiterait de modifier le Code des marchés publics et rajouter cette modalité de participation à la CAO, dans une logique de dématérialisation des marchés publics.

Etendre les modalités de participation à la CAO par vidéoconférence

- Cette intéressante proposition, qui n'entraînerait rien de moins qu'une véritable **remise en cause de la notion de quorum**, permet de réaliser combien les nouvelles technologies impactent désormais le droit des marchés publics, le fonctionnement quotidien de l'administration et de nombreux professionnels du droit.
- Toutefois, il est permis de formuler **quelques réserves** quant à l'instauration de cette proposition, en dehors du coût de ces équipements et de la formation des commissions, qui pourraient constituer le plus évident des obstacles en ces temps de réduction de la dépense publique.
- En effet, à l'usage, ces équipements de vidéoconférences révèlent leurs **limites en présence d'un nombre élevé de personnes**, nécessitent une véritable discipline dans la prise de parole.
- Loin de permettre d'assister à la réunion dans des conditions comparables à une présence physique, ces équipements restreignent au bon vouloir des présents, le champ de vision des vidéoconférenciers.
- Ce dispositif sera-t-il intégré dans la prochaine révision du Code des marchés publics prévue pour 2014 ?

L'enjeu

Promouvoir la dématérialisation et le développement durable, particulièrement dans un département rural.

Il s'agit là d'un enjeu fort au regard du rôle pilote de la commande publique.

(1) [QPF AN n°122566](#),
[Réponse du 22-5-2012](#)

Le CMP

L'article 25 du Code des marchés publics dispose que « *le quorum est atteint lorsque plus de la moitié des membres ayant voix délibérative sont présents* ».

[FRANÇOIS JOUANNEAU](#)



LE JUGE EUROPEEN REAFFIRME LE PERIMETRE DE PROTECTION DES PROGRAMMES D'ORDINATEUR

Tout n'est pas protégé dans un programme d'ordinateur

- Dans une décision du 2 mai 2012 (1), la Grande chambre de la Cour de justice de l'Union européenne a répondu à une **question préjudicielle** sur l'interprétation de la directive 91/250/CEE du 14 mai 1991 (2).
- Cette dernière doit-elle être interprétée en ce sens que la fonctionnalité, le langage de programmation et le format de fichiers de données utilisés dans le cadre d'un programme d'ordinateur peuvent être protégés par le droit d'auteur sur les programmes d'ordinateur ?
- En l'espèce, la société WPL avait acquis une **licence du logiciel SAS** dans le but d'étudier son fonctionnement et de **réaliser un logiciel de substitution**. La société SAS Institute reprochait ainsi à la société WPL d'avoir contrefait son logiciel SAS **en reproduisant ses fonctionnalités**, par l'utilisation du même langage de programmation et du même format de fichiers de données.
- Rappelons que la protection accordée par la directive 91/250/CEE sur les programmes d'ordinateur englobe les formes d'expression d'un programme d'ordinateur ainsi que les travaux préparatoires de conception.
- La CJUE a réaffirmé le principe selon lequel *« ni la fonctionnalité d'un programme d'ordinateur ni le langage de programmation et le format de fichiers de données utilisés dans le cadre d'un programme d'ordinateur pour exploiter certaines de ses fonctions ne constituent une forme d'expression de ce programme et ne sont, à ce titre, protégés par le droit d'auteur sur les programmes d'ordinateur au sens de cette directive »*.

Le code du langage de programmation et du format de fichiers sont protégeables

- La Cour précise toutefois, que la reproduction d'une fonctionnalité par l'utilisation du code relatif à un langage de programmation et/ou à un format de fichiers de données est susceptible de s'analyser comme une contrefaçon.
- Or, en l'espèce, la société WPL avait **observé, étudié et testé le fonctionnement** du logiciel SAS, dont elle avait **acquis légitimement** une licence, pour reproduire la même fonctionnalité par l'utilisation du même langage de programmation et du même format de fichiers de données dans son propre logiciel de substitution.
- Dans la mesure où elle **n'a pas eu accès au code source** du logiciel SAS et elle n'a pas réalisé de décompilation du code objet, son comportement n'est pas susceptible, dans ce cadre de constituer une reproduction partielle du logiciel SAS.
- Dès lors, la fonctionnalité d'un programme d'ordinateur, son langage de programmation et le format de fichiers de données utilisés dans le cadre de ce programme ne sont pas protégeables par le droit d'auteur en tant que tels.
- En revanche, le **code source** et le **code objet** relatifs au langage de programmation et au format des fichiers de données sont **susceptibles d'être protégés** par le droit d'auteur en tant que formes d'expression de ce programme.

L'essentiel

La CJUE réaffirme que les fonctionnalités, le langage de programmation et le format de fichiers de données ne constituent pas une forme d'expression du programme d'ordinateur et ne sont protégés, en tant que tels, par le droit d'auteur.

(1) [CJUE 2-5 2012 Aff.\(C\) 406/10](#).

(2) [Dir. n°91/250/CEE du 14 051991](#).

L'enjeu

La démonstration de la contrefaçon d'un logiciel en raison de la reprise par un tiers d'une fonctionnalité suppose qu'il soit établi une reproduction du code relatif au langage de programmation de ce logiciel.

[ALEXANDRE FIEVEE](#)

[ELENA RODITI](#)



Informatique contentieux

CHARTRE INFORMATIQUE ET LOGICIELS AUTORISES

L'admission de l'audit du poste de travail d'un utilisateur

- Un technicien de maintenance, après avoir reçu un **avertissement** à la suite de la découverte sur le disque dur de son ordinateur professionnel de l'installation de **logiciels non autorisés** par la charte informatique de la société, a été **licencié** suite à la constatation par l'employeur de faits de même nature.
- Le salarié licencié a saisi les prud'hommes de Créteil puis, ses demandes ayant été rejetées, a **saisi la cour d'appel**.
- Ce dernier prétendait dans un premier temps, que l'examen de son ordinateur à l'origine de l'avertissement avait été réalisé en dehors de sa présence et par suite, ne permettait pas le contradictoire. Il demandait donc à ce que le compte-rendu d'audit soit écarté des débats.
- La Cour d'appel de Paris, dans son arrêt du **19 janvier 2012** (1), relève que rien ne vient justifier que le rapport d'analyse produit par l'employeur soit écarté des débats dès lors que l'ordinateur doit être utilisé à des fins strictement professionnelles par le salarié pendant son temps de travail, « *de sorte que l'employeur peut ainsi contrôler cette utilisation hors sa présence* ».

La violation de la charte informatique

- Dans un premier temps, la Cour d'appel de Paris rappelle qu'afin « *d'apprécier la régularité de la procédure et le caractère réel et sérieux des motifs invoqués par l'employeur* », le juge « *forme sa conviction au vu des éléments fournis par les parties* ». La Cour précise que « *si un doute subsiste, il profite au salarié* ».
- En l'espèce, les juges ont constaté que la **charte informatique**, signée par le salarié au moment de son embauche, **interdisait expressément** l'installation de logiciels intrus dans les ordinateurs confiés.
- Les juges ont également rappelé que le salarié avait personnellement été averti à ce sujet, tout comme l'avait été l'ensemble des salariés, par une **note de service** indiquant qu'un incident consistant en une perte de la bande passante l'amenait à procéder à une analyse des logs individuel de la société.
- Enfin, le **contrôle de l'utilisation du réseau internet** au sein de l'entreprise a permis de conclure à une consultation importante en nombre d'octets (195 Mo sur un jour, ce qui correspondait à une consommation supérieure à l'ensemble des autres machines de l'entreprise) de sites manifestement non professionnels, et d'autre part une utilisation d'internet émanant très majoritairement de la machine du salarié.
- La Cour d'appel de Paris a relevé, au regard de tous les éléments qui précèdent, que le salarié avait procédé à un **usage anormal** des possibilités offertes par l'outil informatique confié par l'employeur de nature à **nuire au bon fonctionnement** du système et irrespectueux de la charte signée à cet égard.
- Enfin, la Cour de cassation rappelle que le **règlement intérieur** a également un **pouvoir contraignant**. Il peut en effet contenir des dispositions restreignant le pouvoir de consultation de l'employeur (2). Les sociétés devront donc être particulièrement vigilantes dans la rédaction de leur règlement intérieur.

Les enjeux

La preuve de la violation de la charte informatique peut être obtenue hors la présence du salarié.

(1) [CA Paris, 19-1-2012](#).

Les conseils

Une charte informatique qui détaille très distinctement les logiciels que le salarié peut utiliser sur sa machine professionnelle, ou même le nombre d'octets que le salarié peut consommer par jour avant d'être considéré comme étant une utilisation abusive de son poste de travail, permet à l'employeur de réaliser un audit sur le poste de son salarié sous certaines conditions.

(2) [Cass. soc. 26-6-2012, n° 11-15.310](#).

[MARIE-ADELAÏDE DE
MONTLIVALT-JACQUOT
THOMAS ADHUMEAU](#)



Communications électroniques

ROAMING VOIX ET DONNÉES : NOUVEL ACCORD POUR RÉDUIRE LES PRIX

Nouveaux tarifs de roaming voix et données dans l'UE

- Le coût d'utilisation des téléphones mobiles, smartphones et tablettes lors de voyages au sein de l'Union européenne (UE) baissera fortement à partir du 1^{er} juillet 2012, conformément à un accord provisoire conclu avec le Conseil européen.
- En effet, le Parlement européen a adopté le 10 mai 2012, le **nouveau règlement** sur l'itinérance internationale par 578 voix pour, 10 voix contre et 10 abstentions, entérinant ainsi l'accord politique intervenu fin mars entre la Commission européenne, le Conseil européen et le Parlement européen.
- L'Arcep, aux côtés du gouvernement français et en étroite collaboration avec l'Organe des régulateurs européens des communications électroniques (ORECE), a été activement impliquée dans l'élaboration du nouveau texte.
- La présidence a donné au Conseil européen des informations sur le règlement « itinérance » (10567/12). L'accord politique avec le Parlement européen a été atteint en mars 2012 ; ce dernier a adopté le règlement le 10 mai et le Conseil, le 30 mai (10362/12). Il est en vigueur depuis le **1^{er} juillet 2012**.
- Les modifications apportées au règlement de 2007 (1) vont bénéficier directement aux consommateurs. Les plafonds tarifaires de détail pour les appels émis et reçus et pour les SMS émis en itinérance vont continuer à diminuer jusqu'en 2014.
- Le texte instaure désormais, pour les données en itinérance, un **plafond tarifaire** au détail (et non plus seulement au gros), voué lui aussi à diminuer progressivement jusqu'en 2014. Il permettra ainsi de mettre fin aux factures déraisonnablement élevées à la suite de l'utilisation par le consommateur de données en itinérance.

Stimuler la concurrence sur le marché de l'itinérance

- Les différentes mesures seront particulièrement salutaires en matière de trafic de données. Le coût d'utilisation de tels services sera **plafonné à 70 centimes** d'euro par méga-octet à partir du 1^{er} juillet 2012 et passera ensuite à 45 centimes en 2013, et à 20 centimes dès le 1^{er} juillet 2014.
- En outre, les nouvelles règles permettront aux clients d'acheter des services d'itinérance chez d'autres fournisseurs que leurs fournisseurs nationaux et ouvriront le marché à d'autres fournisseurs, en vue de **stimuler la concurrence** et de **réduire les prix**.
- Le texte prévoit, qu'à partir du 1^{er} juillet 2014, les consommateurs pourront désormais choisir un opérateur différent pour la fourniture de services d'itinérance (mesure dite « de **découplage** »). Il renforce aussi les obligations d'information aux consommateurs.
- Enfin, une obligation de **répondre aux demandes raisonnables d'accès** au marché de gros permettra aux opérateurs, notamment les MVNOs, de construire des offres de tarifs d'itinérance au détail plus intéressantes.
- Dès juillet 2014, les consommateurs pourront **choisir un opérateur différent** de leur opérateur national pour les services d'itinérance. « Ces nouvelles règles contribueront également à l'ouverture du marché pour les nouveaux arrivants et renforceront ainsi la concurrence », a déclaré le rapporteur Angelika Niebler (2).

Les enjeux

De nouveaux tarifs d'itinérance valables en Europe dès 2012 et jusqu'en 2014

(1) Règlement n° 717-2007 du 27 juin 2007.

L'essentiel

La volonté de l'UE est de développer davantage la concurrence sur le marché du roaming pour faire baisser les prix.

(2) Communiqué de presse PE du [8-5-2012](#).

[FREDERIC FORSTER](#)

[EDOUARD LEMOALLE](#)



ACCES AUX DOCUMENTS D'UNE PROCEDURE DE CONTROLE D'UNE CONCENTRATION

L'origine du litige et la décision de refus d'accès aux documents

- En l'espèce, deux sociétés tierces à des opérations de concentration contrôlées par la Commission, l'éditeur français Odile Jacob, dans l'affaire C-404/10 et la société tchèque Agrofert dans l'affaire C-477/10, ont demandé à la Commission l'accès aux documents concernés par les deux procédures de contrôle.
- La Commission a refusé l'accès auxdits documents invoquant la protection des intérêts commerciaux ainsi que les objectifs des activités d'enquête, exceptions au droit d'accès du public aux documents du Parlement européen, du Conseil et de la Commission.
- Saisi par les deux sociétés tierces, le Tribunal a annulé les deux décisions de la Commission jugeant que la Commission avait manqué à l'obligation de démontrer, de façon concrète et individualisée, que ces documents portaient effectivement atteinte aux intérêts protégés par ces exceptions.

L'exception relative à la protection des objectifs des activités d'enquête

- La question se posait alors de savoir si l'expression du refus d'accès à un document dont la divulgation porterait atteinte à la protection des intérêts commerciaux d'une personne physique ou morale déterminée peut être global, par application d'une présomption générale, ou s'il doit être propre à chaque document, ce qui implique un examen concret et effectif de chacun d'eux.
- La Cour procède à un **renversement de la charge de la preuve** par l'instauration d'une **présomption générale** en vertu de laquelle la divulgation des documents échangés entre la Commission et les entreprises au cours d'une procédure de contrôle des opérations de concentration porte atteinte à la protection des objectifs des activités d'enquête et à celle des intérêts commerciaux des entreprises impliquées dans une telle procédure .
- En conséquence, la Commission peut refuser l'accès à tous les documents litigieux afférents aux procédures de contrôle des concentrations, échangées entre la Commission et les entreprises qui notifient ainsi que les tiers, sans procéder au préalable à un examen concret et individuel de ces documents.
- Il appartiendra alors à la personne qui sollicite la divulgation des documents de démontrer l'existence d'un intérêt public supérieur justifiant la divulgation des documents sollicités.
- En revanche, la Cour différencie deux types de documents :
 - les **documents échangés entre la Commission et les parties** qui notifient et entre la Commission et les tiers d'une part ;
 - les **documents internes** de la Commission d'autre part.
- Seule la première catégorie bénéficie de la protection au titre de la non-divulgation aux tiers. La Cour considère en effet que la publication des informations sensibles concernant les activités économiques des entreprises impliquées est susceptible de porter atteinte à leurs intérêts commerciaux, indépendamment de l'existence d'une procédure de contrôle pendante.

Le cadre juridique

- définir les conditions et limites du droit d'accès aux documents du Parlement européen, du Conseil et de la Commission.

- assurer le respect du secret professionnel dans les procédures de contrôle des opérations de concentration entre entreprises.

(1) CJUE 3^e ch. [C-477/10 P](#) et [C-404/10 P](#) du 28-6-2012.

Les fondements de la solution de la CJUE

Les deux règlements 1049/2001 et 139/2004 ne comportent aucune disposition prévoyant la primauté de l'un sur l'autre.

[DIDIER GAZAGNE](#)

[LEILA BENAÏSSA](#)

L'OPPOSABILITE DES CONDITIONS GENERALES D'UTILISATION DE SITES WEB

L'inopposabilité des CGU en l'absence d'offre et de demande

- Les conditions générales d'utilisation (CGU) permettent de définir l'**utilisation autorisée** des contenus du site, la **responsabilité de l'éditeur** du site et les conditions à respecter par les utilisateurs lorsqu'ils peuvent laisser des **contributions personnelles**.
- Il est toutefois nécessaire de s'assurer que ces dispositions ont bien **force obligatoire** par rapport aux personnes visitant et utilisant le site, c'est-à-dire qu'elles leurs soient **opposables**.
- Ainsi, le 23 mars 2012 (1), la Cour d'appel de Paris a jugé que « *le simple fait de se rendre sur un site internet afin de consulter celui-ci sans encore présenter une quelconque demande telle qu'une commande ou une réservation ne saurait engager l'internaute dans des liens contractuels avec la société propriétaire de ce site* ».
- Dans cette affaire, une compagnie aérienne reprochait à une agence de voyage de récupérer sur son site des informations relatives à ses vols, et proposer la réservation de billets depuis son propre site, en violation des CGU de son site web. Ryanair ne peut donc interdire la vente directe de ses billets d'avion en agence sans commettre un acte de **concurrence déloyale**.
- D'après la cour, « *en l'absence, à ce stade de la consultation, de toute demande de la part de l'internaute, et de toute offre de la part du propriétaire du site, il n'existe aucune relation contractuelle* ». Selon la cour, l'internaute ne cochant la **case d'acceptation** des CGU qu'**après avoir sélectionné son vol**, les CGU ne pouvaient donc s'appliquer qu'à l'internaute qui entend conclure avec la compagnie un contrat pour une destination et une date précise.

Comment garantir l'opposabilité des CGU ?

- Il est capital que l'internaute **accepte les CGU**, au stade de **première consultation** du site, c'est-à-dire au moment de l'affichage de la première page sur laquelle il souhaite se connecter. A défaut, rien ne l'empêche de reprendre des éléments qui ne seraient pas protégés par des droits de propriété intellectuelle ou d'en faire des usages illicites.
- La jurisprudence a validé à plusieurs reprises que le système de la **case à cocher vaut acceptation** des CGU.
- L'acceptation expresse par l'internaute des CGU avant même la consultation du site offre une plus grande sécurité juridique. Si une page d'accueil constituée uniquement des CGU ne paraît pas optimale en termes d'attractivité du site, ni même en termes d'efficacité (la première page visitée n'étant pas forcément la page d'accueil) on pourrait cependant envisager l'apparition d'une fenêtre **pop-up** (fenêtre surgissante) à l'ouverture du site, afin que l'internaute ait à accepter les CGU.
- Cette solution permettrait également d'**inclure la demande de consentement** pour l'installation de certains types de **cookies**, imposée par la loi Informatique et Libertés depuis le 24 août 2011.
- Il est par ailleurs recommandé d'intégrer un **lien** vers les CGU dans le **footer** (pieds de page) de toutes les pages du site.
- Une alternative pourrait être d'insérer une **clause** dans les CGU prévoyant leur **application rétroactive** à compter de la première consultation du site.

Les enjeux

La sécurisation d'un site web passe notamment par la rédaction de conditions générales d'utilisation (CGU).

Le simple fait de consulter un site, en l'absence d'offre ou de demande, n'engage pas l'internaute dans des liens contractuels avec la société propriétaire de ce site.

(1) CA Paris 23-3-2012 n° 10-11168 [Opodo c. Raynair](#).

Les conseils

Il est nécessaire d'obtenir l'acceptation des CGU par l'internaute au stade de la première consultation du site.

[MATHIEU](#)

[PRUD'HOMME](#)

[KATHARINA BERBETT](#)



LES COOKIES D'ANALYSE ET DE STATISTIQUES DE FREQUENTATION DES SITES INTERNET

L'implémentation de cookies : entre information et droit d'opposition

- L'ordonnance du 24 août 2011 transposant en France, les directives européennes relatives au traitement des données à caractère personnel et de la protection de la vie privée, prévoit une **obligation de recueil du consentement** de l'internaute s'agissant du stockage d'informations ou de l'accès à des informations déjà stockées dans son équipement terminal. Cette ordonnance est venue modifier l'article 32 II de la loi Informatique et libertés.
- Une **interprétation stricte du texte** conduit à considérer que l'implémentation de cookies d'analyse et de statistiques de fréquentation des sites internet est soumise à l'obligation de recueil du consentement de l'utilisateur.
- La Cnil a d'abord préconisé une application stricte du nouvel article 32 II de la loi Informatique et libertés, pour les cookies d'analyse et de statistiques de fréquentation des sites internet.
- Cependant, après la publication le 10 avril 2012, de l'Union française du marketing direct (UFMD) d'un [guide des bonnes pratiques](#) concernant l'usage des cookies publicitaires, la **Cnil a adapté sa position** aux pratiques relevées sur l'Internet.
- Désormais, la Cnil considère que ces cookies peuvent « être mis en œuvre sans avoir reçu le consentement préalable des personnes concernées » en raison de leur finalité et du risque limité qu'ils font encourir à la vie privée.
- Néanmoins, la Cnil prévoit que l'adresse IP utilisée à des fins de géolocalisation doit être limitée à l'identification de la ville de l'internaute et être supprimée ou anonymisée « pour éviter toute autre utilisation de cette donnée personnelle ou tout autre recoupement avec d'autres informations personnelles ».

Des règles européennes en préparation ?

- A l'occasion d'un **avis du 7 juin 2012** (1) portant sur l'exemption de consentement pour les cookies, le Groupe de l'article 29 (2) se positionne sur la question des cookies d'analyse et de statistiques de fréquentation des sites.
- Les autorités européennes de protection des données ont analysé les **exemptions** à l'exigence de **consentement** et traité le cas des cookies qui, sous certaines conditions, peuvent être placés sans le consentement de l'internaute.
- Le Groupe de l'article 29 explique que bien qu'ils ne relèvent pas de l'exemption conformément au critère de la directive, ils ne sont pas susceptibles de créer un risque pour la confidentialité lorsqu'ils sont strictement limités à une utilisation par « la première partie » (éditeur du site) et lorsqu'ils sont utilisés par des sites web qui offrent déjà des informations claires à ce sujet ainsi que des garanties de confidentialité suffisantes.
- Le Groupe de l'article 29 précise que ces garanties de confidentialité devraient inclure un mécanisme convivial d'opt-out de toute collecte de données et un mécanisme d'anonymisation complet appliquées aux données d'identifications recueillies telles que les adresses IP.
- Enfin, le Groupe de l'article 29 propose l'intégration d'un troisième critère d'exemption au sein de la directive 2002/58/CE, pour les cookies qui sont strictement limités à la première partie anonymisées et agrégées à des fins statistiques.

L'enjeu

Protéger la vie privée des consommateurs... sans ignorer les impératifs liés au développement de l'économie numérique.

- (1) [Avis publié en anglais](#)
- (2) Le Groupe de travail de l'article 29 (institué par la directive 95/46/CE) est composé de représentants des autorités nationales et européennes de protection des données.

Les conseils

Les éditeurs de site doivent faire un audit de leurs politiques cookies pour déterminer les cas exemptés du principe de consentement.

Pour les cookies de fréquentation et de statistiques une analyse fine doit être menée pour déterminer à quel régime ils sont soumis.

[CELINE AVIGNON](#)
[ANAÏS GIMBERT](#)



LE TRAITEMENT D'ANTECEDENTS JUDICIAIRES

Fusion des fichiers STIC et JUDEX

- Un nouveau traitement de données à caractère personnel dénommé « traitement d'antécédents judiciaires » (TAJ) a été mis en place par le décret du 4 mai 2012 (1).
- Ce fichier remplace les deux fichiers d'antécédents judiciaires existants : le **système de traitement des infractions constatées (STIC)** de la police nationale et le **système judiciaire de documentation et d'exploitation (JUDEX)** de la gendarmerie nationale, qui seront définitivement supprimés le 31 décembre 2013.
- Il a en effet pour finalité de « fournir aux enquêteurs de police, de la gendarmerie nationale ainsi que la douane judiciaire une **aide à l'enquête judiciaire** afin de faciliter la constatation des infractions, le rassemblement des preuves de ces infractions et la recherche de leur auteur ».
- Il recense à la fois les **personnes**, majeures ou mineures, **mises en cause** dans une procédure pénale et les **victimes** des infractions.
- Le décret spécifie le **type de données enregistrées** (identité, nationalité, état de la personne, signalement), leur **durée de conservation** (de cinq à quarante ans pour les infractions les plus graves, telles que meurtre viol ou trafic de stupéfiants), ainsi que les **personnes qui peuvent consulter le fichier** (les officiers de police judiciaire, les agents des douanes les magistrats du parquet, notamment).
- Le décret prévoit que toute personne physique identifiée dans le fichier, en qualité de personne mise en cause ou de victime, peut obtenir communication et, le cas échéant, rectification des données la concernant en adressant une demande de **droit d'accès dit « indirect »** à la Cnil, qui effectuera elle-même les vérifications souhaitées.
- Le fichier contient également des informations sur les faits les lieux, les dates de l'infraction et les modes opératoires, ainsi que les données et images relatives aux objets.

Le recours à la reconnaissance faciale

- Le traitement d'antécédents judiciaires utilise un procédé de reconnaissance faciale des personnes **à partir de la photographie** de leur visage.
- Ainsi, les personnes impliquées dans une infraction et dont le visage aura été filmé par une **caméra de vidéoprotection**, pourront être automatiquement identifiées si elles sont déjà connues par les services de police et de gendarmerie.
- Dans son avis du 7 juillet 2011, la **Cnil** considère que :
« cette fonctionnalité d'identification voire de localisation des personnes, à partir de l'analyse biométrique de la morphologie de leur visage, présente des risques importants pour les libertés individuelles, notamment dans le contexte actuel de multiplication du nombre des systèmes de vidéoprotection ».

L'enjeu

Mutualisation du STIC de la police nationale et de JUDEX de la gendarmerie nationale au sein d'un fichier unique d'antécédents judiciaires, dénommé « traitement d'antécédents judiciaires ».

(1) [Décret n°2012-652 du 4 mai 2012](#) pris pour l'application de l'article 11 de la « Loppsi 2 ».

Les perspectives

Il est prévu que les suites décidées par l'autorité judiciaire seront renseignées automatiquement dans le TAJ grâce à une interconnexion avec le traitement CASSIOPEE utilisé par les juridictions.

[VIRGINIE BENSOUSSAN-BRULÉ](#)

LE NOUVEAU CADRE REGLEMENTAIRE APPLICABLE A LA PUBLICITE POUR LES PRODUITS DE SANTE

La publicité à destination des professionnels de santé

- Deux décrets pris en application de la loi relative au renforcement de la sécurité sanitaire du médicament et des produits de santé (1) instaurent le nouveau cadre réglementaire applicable à la publicité à destination des professionnels de santé pour les médicaments à usage humain, ainsi que pour les dispositifs médicaux.
- Directement applicable, le **décret du 9 mai 2012** (2) précise les modalités d'application du régime de contrôle a priori, des publicités pour les **médicaments à usage humain** à destination des **professionnels** de santé instauré par la loi du 29 décembre 2011.
- Les laboratoires doivent dorénavant disposer d'un **visa publicitaire** délivré par l'ANSM avant toute parution. **Quatre périodes de dépôt** de ces demandes de visa sont prévues par an.
- En outre, un mécanisme d'**acceptation tacite** est prévu par le décret aux termes duquel, les demandes de visa « *sont réputées acceptées en l'absence de décision du directeur général de l'Agence dans un délai de deux mois à compter du jour suivant la fin de la période au cours de laquelle elles ont été déposées* ».
- Sous le régime antérieur, ce type de publicité n'était contrôlé par l'Afssaps (devenue ANSM) qu'a posteriori. Seule une dizaine d'entre elles étaient retoquées par an et moins de 20 % faisaient l'objet d'une demande de rectification par l'autorité, aux dires du LEEM (syndicat des entreprises du médicament).
- Les publicités pour les médicaments à usages humain à destination des professionnels de santé se voient donc dorénavant appliquer le régime auparavant exclusivement applicable aux publicités pour les médicaments à usage humain à destination du grand public.

La publicité pour les dispositifs médicaux

- Un second **décret du 9 mai 2012** (3) prévoit une procédure d'autorisation préalable analogue, en ce qui concerne la publicité pour les dispositifs médicaux présentant un risque important pour la santé humaine et dont la **liste est fixée par arrêté** du ministre chargé de la santé.
- Le mécanisme d'**autorisation tacite** en l'absence de réponse de l'ANSM, à l'issue de l'expiration d'un délai de 2 mois à compter de la réception du dossier de demande d'autorisation par l'ANSM, y est repris.
- En revanche, alors que l'autorisation délivrée à l'issue de cette procédure est **valable** 2 ans en ce qui concerne les publicités pour les médicaments à usage humain, la durée de validité de l'autorisation pour les publicités pour les dispositifs médicaux est de **5 ans** à compter de la délivrance du visa.
- Il est également prévu que la publicité pour les dispositifs médicaux, qu'ils présentent un risque ou non pour la santé humaine, devra comprendre un certain nombre de **mentions légales**.
- Enfin, l'entrée en vigueur de ce second décret est différée au **1er janvier 2013**.

L'essentiel

La publicité pour les médicaments à usage humain et pour les dispositifs médicaux présentant un risque important pour la santé humaine sont désormais soumis à autorisation préalable de l'ANSM.

(1) [Loi 2011-2012 du 29-11-2011](#).

(2) [Decr. 2012-741 du 9-5-2012](#).

(3) [Decr. 2012-743 du 9-5-2012](#).

L'enjeu

Les industriels devront dorénavant largement anticiper les publicités des produits qu'ils commercialisent.

[MARGUERITE BRAC](#)
[DE LA PERRIERE](#)
[NICOLAS DUBOSPERTUS](#)



LES SYSTEMES DE TRANSPORT INTELLIGENTS (STI) CODIFIES PAR ORDONNANCE

L'ordonnance crée un article unique dans le Code des transports

- L'ordonnance n°2012-809 du 13 juin 2012 relative aux systèmes de transport intelligents transpose la directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de STI dans le domaine du transport routier et d'interfaces avec d'autres modes de transport.
- Elle codifie les STI à l'article L. 1513-1 du Code des transports dont la rédaction est la suivante :
 - « (...) dispositifs utilisant des technologies de l'informatique et des communications électroniques et mis en œuvre dans le secteur du transport routier et ses interfaces avec d'autres modes de transport pour améliorer la gestion de la circulation, renforcer la sécurité du transport routier, accroître son efficacité en termes d'économie d'énergie et réduire ses effets sur l'environnement et permettre des utilisations plus sûres, mieux coordonnées et plus rationnelles des réseaux de transport (...). »
 - Des spécifications ou normes de conformité et notamment de compatibilité, d'interopérabilité et de continuité des services fournis, seront définies afin d'assurer un déploiement coordonné et effectif des STI dans l'Union. Les spécifications devraient mettre à profit les résultats acquis dans le cadre de l'initiative « eSafety ». Les STI devraient être interopérables et fondés sur des normes ouvertes, publiques et donc accessibles sans aucune discrimination à tous les fournisseurs et utilisateurs d'applications et de services.

Les domaines et actions prioritaires pour le déploiement des STI

- La directive du 7 juillet 2010 a d'ores et déjà défini les domaines et actions prioritaires, qui devraient être repris par le décret.
- **Les domaines prioritaires retenus sont :**
 - l'utilisation optimale des données relatives à la route, à la circulation et aux déplacements ;
 - la continuité des services STI de gestion de la circulation et du fret ;
 - les applications de STI dédiées à la sécurité et à la sûreté routières ;
 - le lien entre le véhicule et les infrastructures de transport.
- **Pour ses 4 domaines, les actions prioritaires établies sont :**
 - la mise à disposition, dans l'ensemble de l'UE, de services d'informations :
 - sur les déplacements multimodaux,
 - en temps réel sur la circulation ;
 - et de réservation concernant les aires de stationnement sûres et sécurisées pour les camions et les véhicules commerciaux ;
 - les données et procédures pour la fourniture d'informations minimales universelles sur la circulation liées à la sécurité routière gratuites pour les usagers ;
 - la mise à disposition harmonisée d'un service d'urgence (eCall) interopérable dans toute l'UE.
- L'accélération du déploiement des STI souhaitée par la Commission est accompagnée d'un plan d'action européen comprenant notamment l'évaluation des aspects relatifs à la sécurité et à la protection des données à caractère personnel liés au traitement des données par les applications et services STI et des problématiques de responsabilité liée à l'utilisation des applications STI et notamment des systèmes de sécurité embarqués.

Les enjeux

Le déploiement des STI contribuera à améliorer :

- les performances environnementales ;
- l'efficacité énergétique ;
- la sécurité et la sûreté du transport routier, et notamment le transport de marchandises dangereuses ;
- la sécurité publique et la mobilité des passagers ;
- la mobilité des passagers et marchandises ;
- la continuité géographique des services STI dans l'Union et à ses frontières extérieures.

L'essentiel

[L'ordonnance du 13 juin 2012](#) transpose la directive du 7 juillet 2010 qui délimite le cadre légal du [plan d'action pour le déploiement de systèmes de transport intelligents en Europe](#) du 16 décembre 2008.

Le domaine d'action n°5 de ce plan d'action a pour objet d'exploiter pleinement le potentiel des STI tout en sécurisant les aspects juridiques tels que :

- les problématiques de sécurité et protection des données personnelles,
- les problématiques de responsabilité liée à l'utilisation des STI.

[DIDIER GAZAGNE](#)
[CAROLINE GOUPL](#)

Noms de domaine

NOUVELLES EXTENSIONS : L'ICANN A DEVOILE LES CANDIDATURES SUR LES NOUVEAUX GTLDS

Près de deux mille demandes d'extensions à analyser pour identifier risques et opportunités...

- Le 13 juin 2012, l'ICANN a dévoilé les **candidatures aux nouvelles extensions** de noms de domaine dont les premières devraient voir le jour au début de l'année 2013. 1930 candidatures dont une cinquantaine de françaises et quelques dizaines de doublons.
- Si l'on retrouve, parmi les candidats, les acteurs incontournables de l'Internet – Google et Amazon regroupent à eux seuls plus de 150 candidatures -, de nombreux titulaires de **marques notoires** dans les domaines allant du luxe à l'industrie en passant bien entendu par les **télécommunications**, cette divulgation révèle de nombreuses candidatures sur des **extensions génériques traduisant l'aspect spéculatif** du projet.
- On peut dès lors s'interroger sur l'avenir d'extensions telles que le « .app » (13 dépôts de dossiers), le .inc (12 candidatures) ou le .home (11 demandes). De même, si ces extensions sont accordées, une **guerre de positionnement** sera sans doute à prévoir entre le .shop et le .store (16 candidatures elles deux) ou encore entre les différents .sex, .porn et autre .adult.
- Enfin, plusieurs demandes d'extensions se rapportant à des communautés pourraient se révéler, pour les personnes concernées particulièrement intéressantes, en termes de développement d'activité sur le web : tel est le cas notamment des **extensions** à connotation **religieuse** (.catholic, .islam), **géographique** (.bzh, .corsica, .NYC) ou **économiques** (.bank, .pharmacy, .insurance).

...et réagir de manière adaptée.

- Les titulaires de droits ayant candidaté étant largement minoritaires, il apparaît aujourd'hui essentiel d'**analyser les candidatures déposées** afin d'identifier une atteinte potentielle à ces droits. Plusieurs voies d'actions sont envisageables : jusqu'au 12 août prochain, l'ICANN permet ainsi de déposer des **commentaires** lesquels seront pris en considération lors de la phase d'évaluation de la candidature.
- Il est également possible, jusqu'au 13 janvier 2013, de **déposer des objections** à une candidature notamment sur le fondement d'une **atteinte aux droits**, du risque de confusion avec une autre extension (**confusion de chaînes**) ou encore l'atteinte à un **intérêt communautaire**.
- Enfin l'ICANN met actuellement en place une Trademark Clearing House, mécanisme ayant pour objet la création d'une véritable **base de données mondiale** permettant d'identifier les **droits à titre de marque**. L'ICANN venant, avec plusieurs mois de retard, de désigner les sociétés en charge de cette mise en place, il conviendra de suivre attentivement les modalités de fonctionnement et de mise en œuvre qui devraient être connus prochainement.
- Concernant les extensions génériques susceptibles de présenter un intérêt, l'analyse et le suivi de ces candidatures devrait constituer une première étape dans la **stratégie de positionnement sur l'Internet de demain**.

Les enjeux

Prévenir les risques liés aux candidatures dévoilées au regard de ses actifs et à ses activités.

Anticiper sa stratégie de développement sur internet face aux autres extensions.

(1) [Communiqué Iccann du 13-6-2012](#).

Les conseils

Identifier les extensions à risque par rapport à ses signes distinctifs et mettre en œuvre les actions adaptées pour faire valoir ses droits.

Identifier les extensions intéressantes par rapport au domaine d'activité ou au secteur géographique et envisager sa présence sur ces extensions.

[VIRGINIE BRUNOT](#)

[ANNE-SOPHIE](#)

[CANTREAU](#)



RACHAT DE SES PROPRES ACTIONS PAR UNE SOCIETE NON COTEE SUR UN MARCHÉ REGLEMENTE

Rappel du dispositif antérieur

- La possibilité pour une société de procéder au **rachat de ses propres actions** a été établie il y a presque 15 ans pour les **sociétés cotées** sur un marché réglementé (1).
- Ce dispositif est également ouvert aux **sociétés non cotées**, mais dans les deux hypothèses suivantes :
 - rachat par la société de ses propres actions suivi immédiatement d'une réduction de capital social non motivée par des pertes ;
 - rachat effectué dans le but d'attribuer les actions aux salariés ou aux dirigeants de la société.
- La **loi de finances rectificative pour 2012** introduit un éventail plus large de possibilités de rachat de leurs propres actions pour les sociétés non cotées sur un marché réglementé (2).

Dispositions introduites par la loi de finances rectificative pour 2012

- Il est désormais possible, pour ces sociétés, de **racheter leurs propres actions** pour les offrir ou les attribuer (3) :
 - **dans l'année** de leur rachat pour des opérations d'actionnariat salarié (dans la limite de 10 % du capital) ;
 - **dans les deux ans** de leur rachat, en paiement ou en échange d'actifs acquis par la société dans le cadre d'une opération de croissance externe, de fusion, de scission ou d'apport (dans la limite de 5% du capital) ;
 - **dans les cinq ans** de leur rachat, aux actionnaires qui manifesteraient à la société l'intention de les acquérir à l'occasion d'une procédure de mise en vente organisée par la société elle-même dans les trois mois qui suivent chaque assemblée générale ordinaire annuelle (dans la limite de 10% du capital).
- L'utilisation des actions rachetées pour une finalité et dans des délais autres que ceux-ci-dessus mentionnés est **sanctionnée** par l'annulation de plein droit des actions.
- La **décision** du rachat d'actions est **prise par l'assemblée générale** ordinaire, laquelle autorise le conseil d'administration ou le directoire à racheter les actions.
- Les **modalités du rachat**, et notamment le prix de rachat sont, quant à elles, **définies par l'assemblée générale** ordinaire. A cet égard, la loi impose l'évaluation des actions par un expert indépendant qui ne fixe pas le prix du rachat, mais donne une fourchette d'estimation de celui-ci.
- La loi dispose enfin que les actions rachetées peuvent être annulées dans la limite de 10 % du capital de la société par périodes de 24 mois, étant entendue que la réduction du capital consécutive à cette annulation doit être autorisée par l'assemblée générale extraordinaire.

Les enjeux

Elargir les possibilités, pour les sociétés non cotées sur un marché réglementé de procéder au rachat de leurs propres actions.

(1) Loi 98-546 du 2-7- 1998

(2) Loi 2012-354 du 14-3-2012, art. 6

(3) C. commerce, art. L. 225-209-2.

Les conseils

Etablir un prix de rachat des actions compris dans la fourchette d'estimation définie par l'expert indépendant.

Le non-respect de cette disposition est en effet sanctionné par la nullité de l'opération.

Prendre garde à ce que cette opération ne porte atteinte, en aucun cas, à l'égalité des actionnaires.

[PIERRE-YVES FAGOT](#)

L'ENCADREMENT DE L'UTILISATION DES NTIC PAR LES FONCTIONNAIRES OU LA E-DEONTOLOGIE

Règles de déontologie en matière d'utilisation des NTIC

- L'introduction des nouvelles technologies de l'information et de la communication (NTIC) concerne aussi bien les entreprises privées que les entreprises publiques. Si les règles d'encadrement de l'utilisation des NTIC par les salariés soumis au droit du travail sont désormais clairement définies, il est intéressant de s'intéresser aux droits et obligations des fonctionnaires en la matière.
- Les fonctionnaires doivent se conformer à leurs obligations déontologiques telles que notamment le devoir d'obéissance, l'obligation de discrétion et de secret professionnel, le devoir de réserve et de neutralité et ce, quelle que soit la situation dans laquelle se trouve l'agent.
- Dans le cadre de l'utilisation des nouvelles technologies de l'information et de la communication, il est alors question d'e-déontologie.

e-déontologie et libertés fondamentales des fonctionnaires : quel arbitrage ?

- Il est recommandé de définir des règles d'utilisation des systèmes d'information au sein de chartes informatiques afin d'être en mesure, le cas échéant de sanctionner les usages non conformes, mais surtout de prévenir les risques liés à cette utilisation.
- Les droits fondamentaux tels que le droit au respect du secret des correspondances prévu par l'article 8 de la Convention européenne des droits de l'homme (CEDH), l'article 10 de la CEDH relatif à la liberté d'expression ou encore l'article 9 du Code civil qui consacre le droit au respect de sa vie privée et au secret des correspondances, constituent les limites nécessaires au pouvoir de l'employeur et notamment en matière de contrôle de l'utilisation des NTIC.
- Il sera nécessaire de trouver un juste équilibre entre les obligations des fonctionnaires au titre de l'e-déontologie et les libertés fondamentales lors de l'établissement de règles d'encadrement de l'utilisation des NTIC.

Les sanctions du non-respect des règles de déontologie

- Le non-respect des obligations déontologiques justifie la prise de sanctions disciplinaires.
- Ainsi, il a été jugé que l'utilisation contraire aux dispositions de la charte informatique et le contournement des mesures techniques de sécurité justifiait l'exclusion compte tenu de la qualité de l'agent et de ses obligations déontologiques de dignité et de loyauté de service (1) ou encore que l'envoi de méls par un agent précisant que les tarifs pratiqués par l'école de commerce sont exorbitants et l'envoi d'informations concernant des formations moins coûteuses portent atteinte à l'établissement qui l'emploie et à l'obligation de réserve de tout agent et justifient sa révocation (2).
- De même, pour le Conseil d'Etat précité, le non-respect d'une charte des systèmes d'information et le contournement de mesures techniques de sécurité justifiait l'exclusion d'un agent compte tenu, en l'espèce, de sa qualité et de ses obligations déontologiques de dignité et de loyauté de service.
- Toutefois, pour être valables, ces sanctions devront être proportionnées aux manquements constatés.

Les enjeux

Encadrer l'usage des NTIC par les fonctionnaires.

- (1) CE, 10-4-2009, [n°312092](#).
(2) CAA Bordeaux, 22-12-2009, [n°08BX02277](#).

Les conseils

- ▶ La définition de règles internes d'encadrement
- ▶ La conciliation entre les libertés fondamentales et la déontologie
- ▶ Des sanctions disciplinaires proportionnelles aux manquements

[EMMANUEL WALLE](#)
[SOPHIE SAVAÏDES](#)



L'hébergement des données de santé : 12 septembre 2012

▪ **Marguerite Brac de la Perrière** animera aux côtés de **François Kaag**, président de l'AFHADS (Association française des hébergeurs agréés de données de santé à caractère personnel), un petit déjeuner consacré au cadre juridique de l'hébergement de données de santé à caractère personnel.

▪ Préalable indispensable au développement de l'e-santé en France, l'hébergement de données de santé à caractère personnel ne peut être réalisé qu'en conformité avec les dispositions du décret n°2006-6 du 4 janvier 2006 et après obtention d'un agrément délivré, pour une durée de trois ans, par le ministre chargé de la santé après avis motivé d'un comité d'agrément et de la Cnil.

▪ A l'heure où la Cnil a annoncé son ambition de multiplier les contrôles auprès des hébergeurs de données de santé, un point sur la réglementation, les bonnes pratiques et les relations contractuelles propres à l'activité d'hébergement s'imposent.

▪ **Inscription gratuite** sous réserve de confirmation avant le 10 septembre 2012 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.

Impact du bilan d'activité de la Cnil sur les entreprises : 26 septembre 2012

▪ **Alain Bensoussan** et **Chloé Torres** animeront un petit-déjeuner débat portant sur l'activité de la Commission nationale de l'informatique et des libertés (Cnil) durant l'année écoulée, c'est-à-dire principalement :

- le fichage et la surveillance en entreprise ;
- le transfert des données personnelles à l'étranger par les entreprises (BRC) ;
- les offres de Cloud computing au regard de la protection des données personnelles et de la sécurité ;
- le lancement des premiers labels Cnil : procédures d'audit de traitements et formations ;
- l'informatisation des dossiers médicaux ;
- l'ordonnance de transposition du Paquet télécoms qui rend compétente la Cnil sur les failles de sécurité.

▪ L'année 2012-2013 s'annonce également riche en actions pour la Cnil, au vu du programme des contrôles annoncés. En effet, la Cnil entend augmenter encore le nombre de ses contrôles, puisqu'elle a décidé d'en effectuer 450 (contre 400 en 2011) sur les thèmes qu'elle juge prioritaires : la vidéoprotection, la téléphonie, la santé, la sécurité, les fichiers du quotidien tenus par les entreprises fournissant des services de première nécessité (eau, gaz, électricité, etc.).

▪ Nous vous proposons, au cours de ce petit-déjeuner, d'aborder les plans de mise en conformité qui s'imposent aux entreprises au vu de l'activité de la Cnil.

▪ **Inscription gratuite** sous réserve de confirmation avant le 24 septembre 2012 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

Google Street View : le Tribunal fédéral Suisse a rendu sa décision

- Le Tribunal fédéral a rendu sa décision le 31 mai 2012 concernant le recours de Google Street View. Selon le tribunal, il n'est pas justifié d'exiger, avant la mise sur Internet, une anonymisation complète des visages et des immatriculations de véhicules sur Google Street View, en plus du floutage automatique (1).
- Il admet dès lors partiellement le recours de la société et précise les exigences pour une **protection efficace** des données dans Google Street View.
- En particulier, il est nécessaire d'**anonymiser** (flouter) « **de manière suffisante** » les images sur lesquelles des personnes ou des plaques de voitures sont reconnaissables.
- Au voisinage des **établissements sensibles** tels que les écoles, hôpitaux, maisons de retraite, centres d'accueil pour femmes, ainsi que les tribunaux et les prisons, une **anonymisation complète** des personnes et des signes distinctifs doit être effectuée.

Calendrier d'application de la loi de protection des données au Mexique

- Le règlement qui complète la Loi fédérale sur la protection des données personnelles détenues par des particuliers (RLFPDPPP) a été publié au journal officiel le 21 décembre 2011.
- Il prévoit qu'au **22 juin 2013**, les responsables de traitements des données personnelles devront :
 - être en conformité avec les dispositions législatives relatives à la sécurité,
 - avoir accomplis les déclarations et mis en œuvre les mesures préventives et correctives.

Droit d'accès à l'information : une loi spécifique en préparation au Maroc

- Une commission interministérielle planche sur le texte de loi, rendu obligatoire par la Constitution marocaine, qui garantirait le droit d'**accès à l'information aux médias**, mais aussi à tout citoyen désireux de savoir ce que fait l'exécutif et d'être informé sur le travail de l'administration.
- Parmi les mesures retenues : un délai à ne pas dépasser pour fournir l'information, un droit de recours contre l'agent qui aura refusé l'information et un organisme pour en accompagner l'exercice.

Etat des lieux sur la loi sur la protection des données à caractère personnel

- La publication de l'identité des **membres de la CNDP** (équivalent de la Cnil française) au Bulletin Officiel a fait courir le délai de deux ans durant lequel les entreprises doivent se mettre en conformité avec la loi marocaine relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel (2).
- Ainsi, toute personne physique ou morale établie au Maroc a **jusqu'au 15 novembre 2012** pour se mettre en conformité avec la loi.



Lexing Suisse

[Sébastien Fanti](#)
actualité du 8-6-2012

(1) Arrêt du 31 mai 2012 ([1C 230/2011](#))



Lexing Mexique

[Langlet, Carpio et associés](#)



Lexing Maroc

(2) Loi n°09-08 et décret n° 2-09-165.

[Cabinet Bassamat & Associée, Fassi-Fihri Bassamat](#)



Traité ACTA : avis défavorable du Parlement européen

▪ Le 21 juin 2012 par 19 voix contre 12, la commission du commerce international du Parlement européen s'est prononcée contre le vote de l'accord commercial anti-contrefaçon (ACTA) (1). C'est dans ce contexte défavorable que le 4 juillet 2012 le Parlement européen en assemblée plénière se prononcera pour ou contre l'accord commercial anti-contrefaçon.

(1) [Communiqué sur traité ACTA, 21 juin 2012.](#)

Harcèlement sexuel : des sanctions aggravées

▪ Le projet de loi relatif au harcèlement sexuel a été déposé au Sénat le 13 juin 2012 (2), tirant les conséquences de la décision du Conseil constitutionnel n° 2012-240 QPC du 4 mai 2012, ayant déclaré l'article 222-33 du code pénal contraire à la Constitution (2). Le nouveau dispositif aggrave les sanctions encourues.

(2) [Projet de loi Enregistré à la Présidence du Sénat, le 13 juin 2012.](#)

Projet de lignes directrices pour les réseaux à haut débit

▪ La Commission européenne invite les parties intéressées à lui présenter leurs observations concernant l'application des règles de l'UE relatives aux aides d'État dans le secteur du haut débit (3).
▪ La principale question soulevée est de savoir comment adapter les lignes directrices actuellement en vigueur aux objectifs de la stratégie numérique de l'UE.

(3) [Communiqué Stratégie numérique sur le tableau de bord 18-6-2012.](#)

Plus de sécurité pour les signatures électroniques transnationales

▪ Le 4 juin, la Commission européenne a publié un communiqué de presse relatif à la signature électronique et au marché du numérique. La Commission propose un nouveau règlement permettant de garantir la sécurité des transactions électroniques transnationales (4).

(4) [Proposition de règlement européen COM \(2012\) 238](#)

Les cartes bancaires de paiement sans contact examinées par la CNIL

▪ Les cartes sans contact (type passe « navigo ») permettent de transmettre des informations entre la carte et un terminal. Pour le paiement de petits achats (inférieurs à 20 €) ces cartes, attractives par leur facilité d'usage ont révélé leur faible sécurité.
▪ La CNIL a décidé de mener des investigations techniques pour analyser les problèmes de sécurité et les conséquences sur la protection de la vie privée (5).

(5) Plus d'informations sur le site de la Cnil, actualité du 10-5-2012.

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

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

Diffusée uniquement par voie électronique – gratuit –

ISSN 1634-0701

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

©Alain Bensoussan 2012



La norme « Coffre-Fort Numérique » : un composant du système d'archivage

Jean-Louis Pascon, Fondateur d'Hénon Conseil et Vice-Président de FedISA (1)

L'AFNOR vient de publier une norme « Coffre-Fort Numérique » : quelle en est la principale avancée ?

La norme est intitulée « Spécifications fonctionnelles d'un Composant Coffre-Fort Numérique (CCFN) destinée à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps ». Derrière ce libellé interminable se cache une avancée pour tous ceux qui souhaitent mettre en œuvre des outils d'archivage numérique sûrs et performants. La norme NF Z42-020 permet aux utilisateurs de systèmes d'archivage d'assurer l'interopérabilité, la réversibilité et l'intégrité des données conservées. Aujourd'hui, les normes existantes sont des normes de conception ou de management ou des normes techniques qui laissent l'utilisateur assez perplexe quant à l'application à des produits ou systèmes existants ou futurs. Cette norme est une brique de base permettant de faire de l'interopérabilité en garantissant les fonctions minimales d'un Coffre-Fort Numérique. Elle est conçue comme un « composant » du système d'archivage permettant aux concepteurs/intégrateurs de logiciels et éditeurs de solutions de partager un minimum commun à tous, de manière à rassurer les utilisateurs d'espaces sécurisés quant à la capacité à fonctionner avec tout produit ou système.

Quels sont les perspectives pour le marché de l'archivage ?

La norme devrait ouvrir le marché puisqu'elle ne contient aucun format propriétaire. Pour les donneurs d'ordre, le choix d'une solution « normée » indépendante de tout produit spécifique est plutôt rassurant et permet un gain de temps dans l'écriture des cahiers des charges. En outre, le fait qu'elle soit « mono tâche » - assurer l'intégrité des Objets Numériques (ON) dans le temps et rien d'autre - est de nature à en faciliter son implémentation. Elle ne traite que des « trains de bits » (les ON) sans se soucier de leur contenu (dossiers administratifs, plans, cartes, factures, vidéogrammes, enregistrements téléphoniques, etc.), ni des formats de fichiers. Elle traite uniquement de la gestion de l'intégrité dans le temps et laisse volontairement de côté toutes les autres considérations (notamment juridiques). Elle décrit ainsi les fonctions de base qui permettent de manier les ON de leur dépôt, jusqu'à leur destruction, en passant par leur contrôle dans le temps. Pour chaque fonction (dépôt, lecture, destruction, contrôle, etc.), sont définis, *a minima*, les paramètres en entrée (par ex. obligatoire/non obligatoire) et ce que doit restituer le coffre en retour.

La norme contient une annexe qui permet de savoir quelles exigences de la NF Z42-013 (2) sur l'archivage électronique (sécurité, horodatage, journalisation, etc.) sont couvertes par le Coffre-Fort Numérique.

Selon vous, quelles évolutions reste-t-il encore à apporter à la norme ?

L'objectif à court terme est de faire de la certification de produits pour assurer une réelle garantie de fonctionnement des coffres. Des discussions sont en cours avec des organismes de certification afin de définir une certification des produits conformément à cette norme. Cela permettra d'avoir des produits constants, capables d'évoluer en fonction des nouvelles versions de la norme. Une autre évolution portera sur les questions de confidentialité pour répondre aux besoins soulevés par la Cnil et l'ANSSI. La norme étant évolutive, il sera possible d'ajouter une couche technique permettant de gérer la confidentialité des données (par des moyens cryptographiques notamment). Cela permettrait d'être en conformité avec le futur règlement européen visant à réformer la directive n° 95/46/CE relative à la protection des données à caractère personnel.

(1) FedISA (Fédération ILM, Stockage et Archivage), www.fedisa.eu

(2) Devenue la norme internationale ISO 14641-1.