Juristendances Informatique & télécoms

Lettre électronique mensuelle réalisée par ALAIN BENSOUSSAN

NUMERO SPECIAL SECURITE

n° 50 – mars 2006

Echanges électroniques et cyber-terrorisme : les chartes d'entreprise sont concernées

Le dispositif législatif issu de la loi Sarkozy

Parmi les mesures concernées par le dispositif législatif issu de la loi du 23 janvier 2006 contre le terrorisme [(1)], celles relatives aux **échanges électroniques** méritent une attention toute particulière : les agents des services de police et de gendarmerie spécialisés peuvent exiger des **entreprises** concernées, la **communication des données de connexion** conservées et traitées par ces dernières.

Cela concerne les **données techniques** (identification des numéros d'abonnement ou de connexion, localisation des équipements terminaux, liste des numéros appelés et appelants, durée et date des communications…) qui peuvent être **exigées en dehors de toute procédure judiciaire** .

Les **entreprises** visées sont désormais toutes celles qui *"au titre d'une activité professionnelle principale ou accessoire, **offrent au public une connexion** permettant une communication en ligne par l'intermédiaire d'un accès au réseau, **y compris à titre gratuit***".

Si les entreprises qui fournissent un accès à l'Internet à leurs employés, sont manifestement exclues du dispositif, il concerne en revanche l'ensemble des espaces, tels que les **cybercafés**, dans lesquels un **accès à l'Internet** est offert à tous, **même à titre accessoire** [(2)].

Les chartes d'entreprise doivent être mises à jour

La question de la **durée de conservation** des données techniques n'est cependant **toujours pas tranchée** dans la mesure où un décret d'application devrait la prévoir.

La France pourrait à ce titre, adosser sa position à celle de la **proposition de directive** relative à la conservation des données du 21 septembre 2005 qui prévoit une **durée d'un an** pour les données de trafic relatives à la **téléphonie fixe** et mobile, et de **six mois pour l'Internet**.

Dès lors, même si les **entreprises** qui procurent un accès à l'Internet à leurs employés ne sont pas directement visées par le texte, il n'en reste pas moins que la durée de conservation des données de connexion au moyen de leurs serveurs de communication devra probablement s'en inspirer.

Elles pourraient **difficilement justifier d'une durée** de conservation **supérieure** à celle nécessitée pour les besoins de la lutte anti-terroriste.

Les enjeux

Se doter des moyens pour lutter contre le terrorisme : vidéosurveillance, échanges téléphoniques et électroniques, nouveaux traitements de données à caractère personnel, procédure pénale et amélioration de l'indemnisation des victimes, gel des moyens de financement.

(1) Loi n° 2006-64 parue au *JO* du 24/01/2006.
(2) Cf. interview p. 11.

Les conseils

Les chartes d'utilisation des systèmes d'information, désormais en pratique obligatoires, ont intérêt à préciser les durées de conservation des données techniques de connexion de leurs personnels. Une révision pourra donc rapidement s'imposer.

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

© Alain Bensoussan - 2006

Informatique

Renforcer sa politique de sécurité : une préocupation constante de l'entreprise

Intégrer une charte dans sa politique globale de sécurité

- Les moyens informatiques et les réseaux de télécoms sont devenus des **outils de travail indispensables** à l'activité quotidienne des entreprises.
- Or, l'utilisation de **systèmes** d'information et de communication **de plus en plus ouverts** avec l'extérieur rend indispensable la mise en œuvre d'une politique de sécurité visant à protéger de risques variés.
- Face aux **nombreuses menaces** et compte tenu des obligations imposées notamment par l'article 35 de la loi Informatique et Libertés (1) applicables à la protection des systèmes et des données nominatives, les entreprises doivent **définir des politiques globales de sécurité**.
- Les **moyens techniques** même s'ils sont indispensables ne sont **pas suffisants** et doivent s'accompagner d'une politique d'**information** et de **sensibilisation des utilisateurs** pour éviter que ceux-ci, par un comportement inapproprié, ne compromettent la sécurité de l'entreprise.
- Ceci explique le **succès grandissant des chartes** depuis quelques années dont la généralisation répond à ces préoccupations.

Compléter la charte par des procédures de constats

- En **complément de la charte** il apparaît nécessaire de définir des **procédures** pour la recherche et la conservation de la **preuve** en cas d'utilisation déviante des systèmes d'information et de télécoms ou encore d'agissement frauduleux avérés.
- Ces procédures doivent permettre de **concilier efficacité et fiabilité des constats** pour que ceux-ci soient juridiquement recevables et probants dans le respect des dispositions édictées par le Code du travail et par la loi Informatique et Libertés qui consacrent des exigences de proportionnalité, de transparence et de loyauté.
- Leur mise en œuvre nécessite par conséquent une **bonne connaissance des textes applicables** et des jurisprudences rendues en ces matières.
- Par ailleurs, il ne faudra pas oublier la **gestion assurantielle des risques** liés à la sécurité résultant notamment de la **perte de chiffre d'affaires** induite par des actes frauduleux ou encore les coûts engendrés par la **reconstitution des données** qui seraient altérées ou perdues.

L'enjeu

Se protéger de risques variés tels la destruction ou la corruption d'informations, l'altération de données, le vol d'informations, l'usurpation d'identité, l'utilisation de ressources ou le dénie de services.

(1) Loi du 06/01/1978 modifiée par la loi du 06/08/2004.

Les conseils

- encadrer les conditions d'utilisation des systèmes d'information par une charte ;
- définir des procédures de constats en cas d'utilisation déviante ;
- prévoir une gestion assurantielle des risques liés à la sécurité.

Pascal Arrigo
pascal-arrigo@alain-bensoussan.com

© Alain Bensoussan - 2006

Communications électroniques

Respecter l'état de l'art en matière de sécurité des systèmes d'information

Du droit à la sécurité vers un droit « de la sécurité »

De la loi Sarbanes-Oxley (SOX), aux accords de Bâle II [2], en passant par la loi de sécurité financière (LSF) [1], sécurité quotidienne, sécurité intérieur, Sarkosy I et la loi sur la protection des données personnelles, on ne compte plus les **dispositifs légaux** et **réglementaires** relatifs à la **sécurité** des systèmes d'information.

Cet afflux de textes montre que cette préoccupation est aujourd'hui prise en compte par le législateur à travers l'élaboration d'un **droit de la sécurité**.

Il est donc nécessaire pour l'entreprise de **connaître** avec précision l'ensemble du **référentiel légal** qui s'applique en matière de sécurité aux informations qu'elle manipule dans son **secteur d'activité** (aéronautique, santé, banque…).

Le **recours aux normes** peut s'avérer indispensable. Si elles ne sont souvent que des **recommandations techniques** sans force obligatoire, leur application devient cependant **de plus en plus courante** au sein des professions, leur conférant ainsi une certaines portée juridique.

Elles sont considérées par le juge comme la **codification écrite** regroupant des « **règles de l'art** » ou des « **usages loyaux et constants** ».

Respecter les normes ISO c'est bien, être certifié c'est encore mieux

A quelle norme se référer pour les SI ? Il existe depuis **octobre 2005** une norme internationale concernant la sécurité de l'information, la **norme ISO/CEI 27001** dont le titre est «Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information – Exigences » [3].

Cette norme représente le **premier cadre normatif** en matière d'organisation et de management de la sécurité des SI. Y faire référence dans un **contrat** par une **clause ISO/CEI 27001** ou en l'intégrant au **cahier des charges** permet de la **rendre obligatoire** entre les parties.

Mais au-delà de cette référence, il s'agit d'une norme qui peut être utilisée dans le cadre d'une **certification** par un **organisme indépendant** et reconnu, qui apporte la garantie-sécurité pour l'entreprise.

La certification, qui est aujourd'hui possible en France, apporte un **atout compétitif**. Il est clair qu'une entreprise sera plus enclin à choisir un partenaire qui a mis en place une procédure de certification, preuve de la **conformité de son SI**.

L'enjeu

Connaître le référentiel légal « sécurité des données » applicable à son secteur d'activité et prendre en compte les bonnes pratiques de la sécurité de l'information.

(1) La SOX a été adoptée le 30/07/2002 par le Congrès américain et la LSF (loi n°2003-706) dont le périmètre est plus large date du 01/08/2003.
(2) Chantier qui va réformer le système international bancaire à l'échéance de 2007.

Les conseils

- Implémenter la norme dans l'entreprise.

- Référencer la norme dans les contrats avec les prestataires et sous-traitants.

- Obtenir la certification ISO/CEI 27001.

(3) Elle définit l'ensemble des tests et contrôles à effectuer pour s'assurer du bon respect d'ISO/CEI 17799.

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

© Alain Bensoussan - 2006

Utilisateurs informatiques

L'audit de sécurité d'un système d'information

La cartographie du SI : un pré-requis à l'audit…

- L'audit de sécurité d'un SI nécessite une **analyse** tant **juridique** que technique et un pré-requis, la cartographie du système d'information.
- Au plan juridique, il faut en effet que l'ensemble des documents associés aux accès au SI et aux usages de l'entreprise soient bien **en conformité avec la réglementation** et les normes en vigueur, notamment en ce qui concerne la charte des utilisateurs tout autant que les contrats avec les prestataires.
- Cela passe donc par l'élaboration d'une cartographie qui **recense l'ensemble des éléments** matériels, réseaux, logiciels installés ainsi que des **flux associés** au SI (usages usuels des mèls, flux de production certifiés), y compris ceux véhiculés à travers les logiciels (type ERP).
- Dans le cadre de ce transfert de flux, il convient de s'interroger sur la **nature des données véhiculées** et sur ce que la cartographie doit répertorier, mais aussi les réseaux sur lesquels ses flux sont véhiculés (lesquels peuvent être soumis à des réglementations étrangères notamment s'ils comportent des éléments transfrontaliers). Certains flux de données sont encadrés de manière différente selon le pays dans lesquels ils sont réalisés.

… pour assurer une parfaite opposabilité du SI

- Après cette première étape de cartographie, il convient de s'assurer de **l'application des éléments de sécurité**. Cela consiste à vérifier que les niveaux de sécurité définis dans la cartographie sont appropriés aux besoins de l'entreprise et qu'il y a bien **accord avec les éléments juridiques et ce notamment en terme de droits d'accès aux informations conservées**.
- Les éléments techniques sont **parfois en écart** avec les éléments juridiques, ne serait-ce que du fait du maintien en conditions opérationnelles du système d'information.
- L'audit de sécurité du système d'information doit permettre d'assurer une parfaite opposabilité du système d'information en toutes ses composantes (flux, données, accès), à des **instances de contrôle** qui pourraient venir réaliser non pas des audits préalables, mais des **audits a posteriori**.
- Ces instance de contrôle ont pour mission de s'assurer notamment de la conformité du système d'information aux **règles comptables**, **fiscales** et autres exigences réglementaires (loi Sarbanes-Oxley, Bâle II, directive européenne sur la protection des données personnelles…) de même qu'**aux usages** qui sont également des contraintes pour une entreprise.

L'enjeu

Gérer et conserver une preuve efficace et pérenne au plan juridique et technique en cas d'intrusions extérieures dans le système d'information, de défaillances ou d'actes de malveillance.

Les conseils

- conserver une définition et un suivi des matériels utilisés et des évolutions du système d'information.
- répertorier tous les modes d'accès internes /extemes y compris les connexions au SI par des systèmes mobiles (portables, ports USB, connexion Wifi, extranet, webmail).
- s'assurer de l'étendue des logiciels installés, des modes d'installation et de fonctionnement (configurations de type client-serveur)
- gérer les flux liés au SI.

Pierre Saurel
pierre-saurel@alain-bensoussan.com

© Alain Bensoussan - 2006

Propriété intellectuelle

La surveillance des marques sur internet : une sécurité contre les atteintes aux droits

L'objectif de la surveillance

Les enjeux

Identifier les tiers qui utilisent les noms de l'entreprise pour favoriser leur propre présence sur le web.

▸ L'internet offre des **possibilités sans cesse nouvelles** d'échanger des informations. Les techniques de **référencement** se sophistiquent, les moteurs de recherche développent des activités publicitaires pour utiliser l'espace dont ils disposent sur leur site, avec en particulier l'offre de positionnement payant de Google, le « **domain name parking** » (1).

▸ Ces nouvelles possibilités vont de pair avec le développement du commerce électronique. Dans ce contexte, il appartient aux entreprises, titulaires de droits de **surveiller l'usage** qui peut être fait des noms sur lesquels elles ont des droits : leur dénomination sociale, nom commercial, enseigne, marques, noms de domaine, mais aussi les droits d'auteur sur le titre de leurs logiciels.

(1) Pratique consistant à enregistrer un nom de domaine et à l'utiliser pour donner accès à un site constitué de liens vers les sites de tiers, avec une rémunération au clic.

▸ La surveillance de l'usage des noms de l'entreprise par les tiers sur le web permet d'optimiser l'efficacité de la présence sur le web, d'éviter les risques de confusion et les **dérives de connexion et d'audience**.

Quelles sont les méthodes de surveillance ?

Le conseil

Mettre en place des techniques de surveillance adaptées aux risques et aux objectifs.

▸ La **surveillance des enregistrements de noms de domaine** peut être automatisée et confiée à un organisme de recherches. Elle permet de relever les enregistrements de **noms de domaine identiques** ou ressemblants à ceux de l'entreprise et, selon l'usage et le titulaire, de décider d'**agir le plus tôt possible** pour une radiation ou un transfert.

▸ La surveillance peut aussi porter sur le référencement des tiers sur le web à partir des noms de l'entreprise. Il s'agit de procéder à des **requêtes sur les noms de l'entreprise** et d'identifier les liens vers les sites des tiers afin d'agir pour faire cesser d'éventuels **liens illicites** par une mise en demeure.

▸ Pour **mesurer les conséquences d'atteintes aux droits** sur les noms, il est important de conserver les statistiques de connexion, d'analyser l'audience et la valeur du clic d'un internaute.

▸ La surveillance, en tant qu'outil de **prévention** permet une action rapide, elle favorise donc **l'efficacité**. Elle s'inscrit dans le cadre plus général de la stratégie de **valorisation des droits** et bien entendu de défense de l'image et des droits.

Marie-Emanuelle Haas
marie-emanuelle-haas@alain-bensoussan..com

© Alain Bensoussan - 2006

Relations sociales

Calcul de l'indemnité de licenciement pour motif économique

Une salariée d'une société en redressement judiciaire, a été **licenciée** par lettre du 2 mai 2002, pour **motif économique**.

La salariée a saisi le Conseil de Prud'hommes d'une demande d'un **complément d'indemnité de licenciement** en se référant au **décret du 3 mai 2002** entré en vigueur le 7 mai qui porte de 1/10ème à 2/10ème de mois de salaire, par année d'ancienneté, l'indemnité de licenciement fondée sur un motif économique.

Les juges du fond ont fait droit à la demande de la salariée considérant que si le droit à l'indemnité de licenciement naît à la date d'effet du licenciement, son montant se calcule à la fin du préavis.

La **Cour de cassation** (1) n'a pas suivi la décision des juges et a considéré que les dispositions du **décret** du 3 mai 2002, entrées en vigueur le 7 mai suivant **ne pouvaient s'appliquer** à l'espèce, celles-ci n'étant pas en vigueur à la **date de notification du licenciement**.

Emploi dissimulé et cumul d'indemnités

Dans 5 arrêts rendus le même jour, la **Cour de cassation** (2) s'est positionnée sur la possibilité, pour un salarié dont l'emploi a été dissimulé, **de cumuler l'indemnité forfaitaire avec d'autres indemnités**.

Dans les 5 espèces, la chambre sociale retient le même **attendu de principe** selon lequel *« les dispositions de l'article L.324-11-1 du Code du travail ne font pas obstacle au cumul de l'indemnité forfaitaire qu'elles prévoient avec les indemnités de toute nature auxquelles le salarié a droit en cas de rupture de la relation de travail, à la seule exception de l'indemnité légale ou conventionnelle ».*

Il n'est donc **plus possible**, pour le salarié dont l'emploi a été dissimulé, de cumuler indemnité forfaitaire et indemnité légale ou conventionnelle de licenciement. Il **doit** désormais **opter** pour l'**indemnisation la plus favorable**.

En revanche, le salarié dont l'emploi a été dissimulé, **peut cumuler** l'indemnité forfaitaire avec :

- l'indemnité compensatrice de préavis,
- l'indemnité pour non-respect de la procédure de licenciement,
- l'indemnité de congés payés,
- l'indemnité pour licenciement sans cause réelle et sérieuse,
- les dommages et intérêts pour violation de l'ordre des licenciements.

Extraits

« Attendu que le droit à l'indemnité de licenciement naît à la date où le licenciement est notifié et que ce sont les dispositions légales ou conventionnelles en vigueur à cette date (date de la notification du licenciement) qui déterminent les droits du salarié (…) ».

(1) Cass. soc. 11 janv. 2006, n°03-44.461.

« Aux termes de l'article L.324-11-1 C. trav., le salarié dont l'emploi a été dissimulé a droit, en cas de licenciement, à une indemnité forfaitaire égale à 6 mois de salaire, à moins que l'application d'autres règles légales ou de stipulations conventionnelles ne conduise à une solution plus favorable ».

(2) Cass. soc. 12 janv. 2006, 5 arrêts n°04-42.190, 04-43.105,04-40.991,03-46.800,04-41.769.

Pierre-Yves Fagot
pierre-yves-fagot@alain-bensoussan.com
Céline Attal-Mamou
celine-attal-mamou@alain-bensoussan.com

© Alain Bensoussan - 2006

Pénal numérique

L'extorsion des données personnelles à la recherche de sa qualification pénale

Le « phishing », une technique de fraude

L'enjeu

Usurper l'identité virtuelle (marque, logo ou couleurs) de sociétés importantes pour collecter des éléments d'identification d'internautes peu méfiants.

Un jeune internaute avait **imité la page** permettant de s'enregistrer à Microsoft **MSN Messenger** sur un site personnel de sa création. Les internautes désireux de s'abonner à ce service étaient alors amenés sans le savoir à **livrer leurs données personnelles** à ce dernier, à l'adresse électronique spécialement créée à cet effet.

Il se livrait ainsi à une pratique bien connue de l'internet : le **phishing**, récemment traduit officiellement en « **filoutage** » ou « hameçonnage » et défini comme la « ***technique de fraude*** *visant à obtenir des informations confidentielles, telles que des mots de passe ou des numéros de cartes de crédit, au moyen de messages ou de sites usurpant l'identité d'institutions financières ou d'entreprises commerciales* » (1).

Cette pratique soulève toutefois d'importantes difficultés de **qualification juridique**. C'est la deuxième fois que le Tribunal de grande instance de Paris est amené à se pencher sur la question.

Il l'a fait la première fois en septembre 2004 en jugeant que la **création de sites miroirs** copiant des sites existants de banques françaises afin de recueillir des informations confidentielles émanant de leurs clients internautes constituait le délit d'**escroquerie** (2). Le prévenu avait alors été condamné à la peine d'un an de prison et à indemniser le préjudice subi.

(1) Avis paru au JO du 12/02/2006.
(2) TGI Paris, 13ème ch. 02/09/2004.

Une pratique condamnable à plus d'un titre

Les conseils

Vérifier, dans la barre d'adresse du navigateur, l'adresse du site internet avant de saisir une quelconque information.

Le dernier jugement se prononce en faveur de la **contrefaçon par copie servile** de la page d'enregistrement à MSN (3). Le prévenu a été jugé coupable de détention de produits revêtus d'une **marque contrefaite** utilisée sans autorisation, de contrefaçon par édition ou reproduction d'une oeuvre de l'esprit au mépris des droits de l'auteur et de contrefaçon par diffusion ou représentation.

En revanche, jugeant que le dispositif mis en oeuvre était de « mauvaise qualité » et que l'efficacité de celui-ci n'était pas démontrée, le tribunal, retenant en outre l'âge du prévenu et l'absence d'antécédents judiciaires, l'a condamné à une **peine** bien plus **légère** de 500 euros avec sursis.

Cette décision constitue un nouvel et bel exemple de l'adaptation du droit pénal aux évolutions technologiques et à la créativité de l'humain

Même si **d'autres qualifications** pénales paraissent envisageables, aux côtés de l'escroquerie et de la contrefaçon, comme la **collecte déloyale** de données nominatives, force est de reconnaître que loin de se heurter à un vide juridique, la poursuite et la sanction du « phishing » paraîsent plutôt facilitées par une large option entre **différents textes répressifs**.

(3) TGI Paris, 31ème ch., 21/09/2005, Microsoft Corporation c. Robin B.

Anne Cousin
anne-cousin@alain-bensoussan.com

© Alain Bensoussan - 2006

Fiscalité et société

Tenue des comptabilités informatisées : la sécurité avant tout !

La nouvelle instruction fiscale du 24 janvier 2006

L'enjeu

Les manquements aux obligations de conservation et de présentation sont susceptibles de conduire au rejet d'une comptabilité informatisée.

▸L'évolution des **matériels** et des **logiciels** mis à la disposition des entreprises pour la tenue de leur **comptabilité** a conduit l'administration à préciser les obligations fiscales et comptables des entreprises dans une **nouvelle instruction du 24 janvier 2006**(1) qui se substitue à ses deux précédentes instructions (2).

▸Cette nouvelle instruction **rappelle** le **cadre juridique** du contrôle des comptabilités informatisées en énonçant les **principales règles** afférentes à la tenue d'une comptabilité informatisée, sincère, régulière et probante, conformément au plan comptable général révisé de 1999 :

- intangibilité des écritures après validation,
- numérotation chronologique,
- permanence du chemin de révision entre l'écriture et la pièce justificative qui en est à l'origine.

▸Le **périmètre du contrôle** des comptabilités informatisées **s'étend** notamment **aux données** qui concourent indirectement aux écritures comptables issues du domaine de gestion auquel les entreprises recourent de plus en plus pour le suivi, par exemple, **de la facturation ou de la production**.

(1) BOI n°13 L-1-06.
(2) BOI n° 13 L-6-91 et n° 13L-9-96.

Sécurité juridique rime avec sécurité des systèmes d'information

Les conseils

- Réaliser des archivages mensuels ou trimestriels ;

- Disposer d'un dispositif sécurisé de création de signature électronique qui soit certifié.

▸L'instruction fiscale précise que la mise en place de la **traçabilité** d'éventuelles modifications des données, ainsi que le recours à la **signature électronique** pour renforcer le caractère incontestable de l'archivage effectué sont de nature à garantir aux entreprises qu'elles se conforment à leurs obligations de conservation.

▸La **procédure d'archivage** qui intervient lors de la clôture de l'exercice ou de la période comptable, doit être distinguée de la **procédure de sauvegarde** dans la mesure où une sauvegarde ne permet pas toujours de satisfaire aux **obligations de conservation** définies par les textes.

▸Le **format type** des copies de fichiers accepté par l'administration est précisé pour tenir compte des **évolutions technologiques**.

▸L'instruction rappelle les différentes modalités du **contrôle** des comptabilités informatisées à la lumière de la jurisprudence du Conseil d'Etat (3) et les comportements de nature à constituer une **opposition** au contrôle fiscal et à entraîner une **évaluation d'office** des bases d'imposition.

(3) CE 5 mai 1999, n° 197379 (SA Ardex) - CE 16 juin 2003, n° 236503 (SARL Le Veneto).

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

© Alain Bensoussan - 2006

Collectivités territoriales

La sécurité dans le processus de dématérialisation des achats publics

Les étapes préalables à la dématérialisation des procédures

L'enjeu

Anticiper l'ensemble des risques liés à la dématérialisation des achats publics avant la mise en place de la plate-forme par la collectivité territoriale.

- **L'article 56** du Code des marchés publics oblige les acheteurs publics à prendre toutes les mesures nécessaires pour la **réception des candidatures et des offres par voie électronique**.
- Comme le démontre le « **Guide technique pour la sécurité** de la dématérialisation des achats publics » (1) élaboré sous l'égide du Ministère de l'Economie et des finances, cette dématérialisation implique une étude préalable de l'ensemble des problématiques inhérentes à la **sécurité de la future plate-forme**.
- Un **audit préalable des besoins en sécurité** informatique doit donc être effectuée par la collectivité avant la mise en place de sa plate-forme dématérialisée.
- A ce titre, la personne publique doit par exemple **quantifier ses besoins** en termes de **confidentialité et d'intégrité** des informations, de **disponibilité des systèmes**, d'opposabilité des procédures internes ou encore, de **traçabilité** des actions menées.

(1) Guide à consulter sur : http://www.men.minefi.gouv.fr/webmen/themes/adm/recommandations.doc.

Les mesures de sécurité des candidats et acheteurs publics

Le conseil

Le candidat doit notamment acquérir un certificat de niveau 2 et contrôler que sa candidature et/ou son offre ne contient aucun virus

L'acheteur public doit prendre toutes les dispositions nécessaires (mise à jour régulière du pare-feu, mise d'un système de détection d'intrusion…) pour sécuriser sa plate-forme de dématérialisation.

- Il est demandé aux candidats d' **acquérir un certificat électronique au minimum de « niveau 2 »** auprès d'un prestataire référencé, puis de contrôler que les certificats ne seront utilisés que par leurs **seuls titulaires**. Ils doivent en outre vérifier, avant l'envoi de leurs candidatures et de leurs offres, que les pièces qu'ils transmettent ne contiennent **pas de virus**, puisque la présence d'un virus est susceptible d'entraîner l'élimination d'office du candidat.
- L'**acheteur public** doit quant à lui, prendre deux types de mesures.
- Tout d'abord, des mesures de **sécurisation de la plate-forme** de dématérialisation, afin que celle-ci permette de manière sûre d'**horodater** et de tracer toutes les actions, tout en garantissant l'**intégrité** et l'origine des documents. La mise en place et la mise à jour d'un pare-feu, d'un **système de détection d'intrusion**, d'un anti-virus ou encore d'un certificat de serveur sont par exemple primordiales.
- Ensuite, d'un point de vue **organisationnel**, tous les **agents publics** intervenant en matière de marchés dématérialisés **doivent être identifiées** et leurs rôles strictement délimités. L'accès des agents aux marchés dématérialisés doit faire l'objet d'un contrôle transparent, en vue de démontrer, le cas échéant, que toutes les précautions ont été prises, par exemple lors de la phase d'ouverture des candidatures et des offres.

Arnold Vève
arnold-veve@alain-bensoussan.com

© Alain Bensoussan - 2006

Actualité

Les téléservices sont en marche

Un **projet de loi ratifiant l'ordonnance** du 8 décembre 2005 relative aux **échanges électroniques** entre les usagers et les autorités administratives et entre les autorités administratives a été présenté lors du conseil des ministres du 22 février [1] afin d'écarter la caducité de l'ordonnance.

Ses dispositions vont donc être totalement applicables en particulier celles établissant l'**équivalence juridique** entre le **courrier électronique** et le courrier sur support **papier** et prévoyant que la **saisine de l'administration par voie électronique** est régulière et doit faire l'objet d'un accusé d'enregistrement informant l'usager que sa demande a été prise en compte.

Les sources

(1) http://www.premier-ministre.gouv.fr/

Phishing ou filoutage : une forme d'escroquerie sur internet

La Commission de néologie chargée du vocabulaire de l'internet a préféré retenir le terme de « **filoutage** » pour traduire « **phishing** » tout en reconnaissant que le terme « **hameçonnage** » est aussi en usage[2].

Quoiqu'il en soit, ces pratiques sont des **techniques de fraude par courriel** fondées sur l'usurpation d'identité.

(2)Avis du *JO* du 12/02/2006

Comité d'agrément des hébergeurs de données de santé

La **composition** du comité d'agrément des hébergeurs de données de santé à caractère personnel a été fixé par l'arrêté du 7 février 2006[3].

Ce dernier **examine les garanties** d'ordre éthique, déontologique, financier et économique qu'offre le candidat «hébergeur » avant de se voir délivrer un agrément pour une durée de trois ans.

(3) *JO* du 15/02/2006

Charte pour un développement responsable du multimédia mobile

Le **ministre délégué à la Sécurité sociale**, aux Personnes âgées, aux Personnes handicapées et à la Famille et les sept opérateurs membre de l'**Association française des opérateurs mobiles** (Afom) [4] ont signé le 10 janvier, une charte pour un développement responsable du multimédia mobile.

Il pourra être fait référence à cette charte dans le cadre des contrats conclus avec les opérateurs.

(4) Bouygues Télécom, Orange, SFR, Débitel, M6 Mobile, Omer Télécom et Universal Mobile.

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

© Alain Bensoussan - 2006

Interview

Développer des dispositifs de « surveillance opérationnelle » des échanges électroniques

Mr Jean-Claude TAPIA, Président de la société ARSeO (*),

par Isabelle Pottier

En quoi consiste exactement l'activité de votre société ?

Arseo a pour vocation d'aider les entreprises à donner une réalité à un concept de sécurité dynamique qui présume la création de « périmètres de confiance » délimités et maîtrisés. Aussi, avons-nous orienté nos activités de conseil et d'audit vers la valorisation des actifs matériels et immatériels (les identifier, calculer leur valeur, déterminer ce qu'ils représentent pour chaque partenaire et agresseur potentiel), la gestion des risques opérationnels (par processus / activité évaluer les enjeux liés aux ressources utilisées, identifier les situations de risque potentielles, mesurer le degré d'exposition aux risques, déployer les plans de réduction, organiser la gestion des risques), la sécurité des systèmes d'information (définir la politique de sécurité et ses modalités de déploiement, cartographier les menaces et vulnérabilités, auditer les dispositifs, définir les solutions, mettre en place les indicateurs, sensibiliser et former) et la gestion de crise (structurer la veille, la surveillance et la logique d'escalade, former et tester la capacité de réaction).

La loi Sarkozy va-t-elle développer de nouvelles pratiques sécuritaires des entreprises ?

La loi du 23 janvier 2006 oblige les entreprises qui offrent un accès internet, même à titre accessoire, de conserver les traces informatiques des communications électroniques dans le cadre de la prévention du terrorisme. Elle élargit les possibilités offertes en matière d'accès aux données personnelles et techniques issues de l'utilisation des systèmes d'information. En cela, elle modifie sensiblement les finalités primaires des entreprises en matière de gestion des traces (garantir une « utilisation normale » des ressources, détecter toute anomalie pouvant engager la responsabilité de l'entreprise, anticiper les dysfonctionnements et pouvoir en analyser les causes) et étend le périmètre des entités devant être à même de répondre à toute réquisition officielle. Les entreprises concernées vont devoir développer des dispositifs de « surveillance opérationnelle ».

Mais la loi reste imprécise sur certaines questions : quelles informations conserver et combien de temps ? comment financer les moyens nécessaires au stockage et à l'exploitation des données ? comment informer les parties prenantes (clients, partenaires, collaborateurs…) ? comment fiabiliser les dispositifs de collecte face aux outils préservant l'anonymat des transactions (système TOR, usurpations d'identités via le WiFi…) ? comment empêcher toute utilisation frauduleuse ou déloyale des dispositifs mis en œuvre? quels aménagements apporter aux règlements intérieurs et aux chartes d'utilisation des moyens informatiques et de communication ? Les réponses à ces questions constituent autant de contraintes que d'opportunités pour les entreprises et les acteurs en charge de protéger les actifs matériels et immatériels.

Avez-vous quelques conseils pour la mise en place d'une stratégie sécurité ?

Cibler les actifs les plus sensibles. Englober prévention et protection dans un concept plus large qui inclut gestion des risques, sûreté des biens et des personnes, sécurité des SI, veille concurrentielle, conformité, lutte contre les mécanismes frauduleux... Considérer la sécurité comme un geste professionnel que chaque personnel doit mettre en œuvre. Valoriser les comportements sécuritaires et légitimer les métiers de la sécurité. Prendre en compte l'impératif de sécurité dès les premières phases de chaque projet pour optimiser les dépenses, privilégier la prévention et augmenter l'efficacité des dispositifs. Piloter chaque action de sécurisation par les délais et les coûts et identifier les indicateurs permettant de suivre les objectifs atteints. Enfin, comme le font les grands groupes étrangers, coordonner davantage les initiatives privées avec l'action des pouvoirs publics en multipliant les zones de concertation.

(*) http://www.arseo.com/

© Alain Bensoussan - 2006