A quand une législation protégeant le secret des affaires ?

 Le projet de loi pour la croissance, porté par Emmanuel Macron, ne comportera pas de volet sur le secret des affaires.

La législation sur le secret des affaires a en effet été retirée du projet de loi Macron actuellement en discussion à l'Assemblée nationale car jugée attentatoire à la liberté de la presse et aux lanceurs d'alerte.

La France ne disposera pas d'une législation nationale protégeant le secret des affaires, contrairement aux préconisations de l'article 39 du traité ADPIC issu la convention de Marrakech de 1994 qui a institué l'Organisation mondiale du commerce (OMC).

Cette législation prévoyait de punir quiconque prend connaissance, révèle sans autorisation ou détourne toute information protégée à ce titre d'une peine de trois ans d'emprisonnement et de 375 000 euros d'amende.

D'autres pays disposent déjà d'un dispositif juridique comparable. Il en est ainsi aux Etats-Unis où le « Economic Espionage Act » de 1996, plus connu sous le nom de Cohen Act de 1996, répond à ces exigences, tandis que pour l'Union européenne, une proposition de directive sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, devrait être examinée au Parlement européen.

Le volet sur le secret des affaires qui figurait dans le projet de loi pour la croissance, porté par Emmanuel Macron, avait pourtant été amendé lors de la discussion parlementaire pour apporter des garanties aux journalistes craignant pour la liberté de la presse.

Un amendement précisait en effet que le secret des affaires ne s'appliquait pas à la révélation d'une information « strictement nécessaire à la sauvegarde d'un intérêt supérieur, tel que l'exercice légitime de la liberté d'expression ou d'information ou la révélation d'un acte illégal ».

De plus, un autre amendement prévoyait d'insérer la notion de secret des affaires dans la loi sur la presse de 1881, la plaçant au même niveau que celle de « secret professionnel ». Ainsi, les lanceurs d'alerte auraient été protégés.

Mais ces amendements n'ont pas calmé les craintes des journalistes et des lanceurs d'alerte, qui critiquent une définition trop large du secret des affaires et des garde-fous insuffisants.

Le député Richard Ferrand suggère que « ce qui doit être protégé dans la vie des entreprises » soit rediscuté dans le cadre du projet de loi dont il est le

rapporteur sur la protection des sources des journalistes et qui doit être débattu cette année à l'Assemblée nationale (1).

Rien n'est moins sûr car le projet de texte n'a pas bougé depuis plus d'un an. En outre, le texte a pour ambition de conférer un niveau élevé de protection du secret des sources, ce qui n'est pas facilement conciliable avec le secret des affaires….

Pour l'heure, il n'y a pas en France de secret des affaires faute d'une législation protégeant les entreprises de l'espionnage industriel.

Didier Gazagne
Lexing Droit Intelligence économique
Isabelle Pottier
Lexing Droit informatique

(1) Projet de loi 1127, déposé le 12 juin 2013.

Failles de sécurité : quel régime juridique ?

Quel est le régime juridique des failles de sécurité ? Chloé Torres répond aux questions de la rédaction de La Semaine juridique. Mais que recouvre exactement l'expression « faille de sécurité » ?

Quelles sont les obligations légales et en quoi consiste votre intervention ? Quelles sont les tendances ?

L'expression « failles de sécurité » est régulièrement utilisée par les médias qui se font l'écho de comptes clients dérobés lors d'attaques informatiques ou dévoilées sur Internet en raison d'une mauvaise configuration d'un site web. Cette expression recouvre tous les éléments qui portent atteinte à un système de traitement automatisé de données : les erreurs, les bugs mais aussi les fraudes internes et externes. Elle traduit le fait qu'à un instant des données à caractère personnel se trouvent avoir été corrompues.

L'article 34 bis de la loi Informatique et libertés utilise la terminologie de « violation de données personnelles » définit de manière extrêmement large comme toute destruction, perte, altération, divulgation ou accès non autorisé à des données.

L'entreprise victime d'une faille de sécurité doit mettre en place une cellule de crise habituellement composée de la Direction des systèmes d'information (DSI), du responsable de la sécurité des systèmes d'information (RSSI), de la direction

juridique et d'un avocat spécialisé. Cette cellule de crise est chargée de piloter les principales actons (audit de sécurité, dossier de preuve technique, stratégie de communication vis-à-vis de la Cnil et des médias, assurance, etc.).

La proposition de règlement européen sur la protection des données qui devrait être adopté fin 2015 début 2016 va étendre à l'ensemble des entreprises l'obligation de notifier auprès de la Cnil toute violation de données à caractère personnel. Un texte qui aura un impact sur de nombreuses activités économiques…

Chloé Torres, « 3 questions : Failles de sécurité : quel régime juridique ?« , La Semaine Juridique – Entreprise et Affaires, n° 4, 22 janvier 2015.

Piratage des serveurs de Sony Pictures aux Etats-Unis

Piratage des serveurs de Sony Pictures aux Etats-Unis. Alain Bensoussan, avocat spécialisé en sécurité informatique et en intelligence économique répondait aux questions de Wendy Bouchard et des auditeurs sur Europe*1*.

La Maison Blanche parle d'une grave affaire de sécurité nationale. Sony a décidé de ne pas sortir son film « The interview », une comédie sur deux agents de la CIA qui ont pour mission d'assassiner le dictateur Nord Coréen après avoir reçu des menaces d'attentat via un message anonyme. C'est une première.

Europe Midi : Pourquoi La Maison Blanche est-elle si alarmiste alors qu'il ne s'agit pas à proprement parler de piratage de données gouvernementales ?

AB : « *ce sont des données sensibles d'une entreprise à forte visibilité et avec cette affaire, on voit apparaître une nouvelle forme de guerre d'un Etat contre une entreprise privée mondialement connue. De telles entreprises orientées vers un marché de secteur privé ne sont pas capables de lutter contre des forces aussi importantes que sont des forces nationales numériques*« .

Europe Midi : On parle de Sony, mais est-ce que toutes les entreprises y compris les entreprises françaises sont menacées et sont régulièrement soumises à ce type d'attaque informatique ?

AB : « *Pour ce type d'attaque effectivement, il y a très peu d'entreprises françaises qui sont capables de résister d'abord parce-qu'elles ne disposent pas d'un niveau de protection du type de ceux mis en place pour les centrales nucléaires. Pourquoi des entreprises de marché qui ont des clients notamment dans les média, mettraient-elles un tel niveau de sécurité contre ce type d'attaque totalement disproportionné ? Elles ne sont pas du tout préparées à faire face à*

de tels risques« .

Europe Midi : Quels sont les secteurs d'activité en France le plus touchés par le piratage ?

AB : « *Ce sont tous les secteurs où il a des possibilités d'obtenir de l'argent extrêmement rapidement, à travers des atteintes à la vie privée par le piratage des messageries, des détournements de fonds par le phishing. De manière générale, l'obtention de produits sans argent est une délinquance qui se généralise. Ce phénomène s'explique tout simplement parce qu'il est très facile aujourd'hui de se procurer sur le net des outils d'attaque, ces formes de virus sont autant de kalachnikov « binaires », très faciles à utiliser et à la portée de n'importe quel apprenti pirate digital qui peut se transformer en James bond de l'informatique*« .

Europe Midi : On parle de délinquance d'Etat, mais ce ne sont pas les Etats qui s'espionnent. Ils recrutent des pirates informatiques (hackers) pour attaquer des entreprises à capital stratégique.

AB : « *La plupart des Etats disposent d'une « cyberdéfense », c'est-à-dire d'armées numériques de très haut niveau. Personne ne peut ignorer les attaques par virus informatique et la menace s'aggrave chaque jour*« .

Europe Midi : On a besoin de mieux comprendre comment s'armer. Sony a reculé face aux pirates informatique, est-ce la porte ouverte au chantage médiatique ?

AB : « *Ce sont tous les actifs de Sony qui sont en jeu mais il y a aussi les dommages collatéraux et notamment tous les accords que Sony a pu signer avec d'autres entreprises qui sont susceptibles d'être mis à la disposition de tous. On peut comprendre que Sony ait préféré reculer dans un premier temps*« .

Europe Midi : Faut-il abandonner nos ordinateurs et nos connexions à internet en dépit des antivirus ?

AB : « *Les innovations technologiques ont toujours été accompagnées de délinquance. Cela doit entraîner une triple réponse, d'abord pédagogique pour que les utilisateurs cessent d'être négligents sur la sécurité (par exemple, avoir des mots de passe supérieur à 8 caractères avec de l'alpha numérique et des caractères spéciaux). Il faut aussi amener les entreprises à augmenter leur niveau de sécurité et enfin, changer l'arsenal répressif français. Les peines de prison sont de 3 ans et ont été pensées en 1988 sous la loi Godfrain. Aujourd'hui, compte-tenu de la généralisation de ce type de délinquance, il faut sans doute multiplier les peines par 3 ou par 4 afin que le seuil soit plus dissuasif*« .

Europe Midi : Ce qui se passe avec Sony est très alarmant car cette attaque aurait passée 90% des défenses numériques du gouvernement. Ce qui veut dire que que l'on a beau avoir un système de sécurité en béton, il y aura toujours un pirate qui trouvera la faille. C'est à l'évidence ce qui s'est produit ici.

AB : « *Ce qui compte c'est le degré de confiance d'une économie numérique comme la notre. Il faut certes augmenter le niveau de protection, mais contre une attaque de type « cyber guerre », la solution ne peut venir du marché. Dans l'affaire Sony, c'est à l'Etat américain d'apporter une réponse. Par contre, les entreprises doivent néanmoins augmenter leur niveau de sécurité parce que*

derrière les informations moins importantes que celles de Sony, il y a notre intimité et notre vie privée qui doit être assurée« . (…)

Le Journal de Wendy Bouchard sur Europe*1*, Europe Midi en duplex depuis La Roche sur Yon, le 19-12-2004 (Ecoutez l'émission à 38:00 > 45:30).

Confiance numérique : organisation d'un petit-déjeuner débat

Confiance numérique. Polyanna Bigle a participé, le 20 novembre 2014, à un petit-déjeuner débat organisé par CCM Benchmark, en partenariat avec Dictao, sur le thème « Confiance numérique et transformation digitale ».

Les thématiques d'intervention étaient les suivantes :

- l'identité numérique professionnelle au cœur de la digital workplace ;
- l'Imprimerie Nationale et l'identité professionnelle ;
- la sécurité et la confiance des services numériques.

Ces interventions ont permis d'apporter des réponses concrètes aux questions suivantes :

- Quels sont les services liés à l'identification et l'authentification des utilisateurs ?
- Comment établir une relation sécurisée et « de confiance » ?
- Quel est le contexte juridique ?
- Comment déployer un tel système ?
- Quels sont les facteurs clés de succès ?

Des échanges avec les participants ont ponctué ce petit-déjeuner débat sous forme de questions-réponses.

USB : impact des failles des sécurité pour l'entreprise

 **USB.** Katharina Berbett précise, pour Stratégie internet, la

stratégie de protection juridique à adopter en vue de protéger les systèmes d'information de l'entreprise de l'exploitation frauduleuse d'une faille de sécurité.

La découverte d'une importante faille de sécurité de l'USB, baptisée « BadUSB », par deux chercheurs en sécurité informatique allemands, présentée à la conférence Black Hat à Los Angeles en août dernier, suscite de nombreuses inquiétudes. L'exploitation de cette faille, liée à l'absence de protection interne des firmware de périphériques USB, en particulier des clés USB permettrait potentiellement l'intrusion dans un système infecté, le vol d'informations stratégiques ou encore de données à caractère personnel (dont la sécurité est une obligation légale lourdement sanctionnée).

Pour l'heure, il n'existerait pas de protection technique efficace. C'est pourquoi, pour pallier cette vulnérabilité, la mise en place d'une protection juridique est nécessaire et peut être l'occasion de revoir la sécurisation de ses systèmes, mais aussi de développer ou d'étendre l'utilisation de plateformes et d'outils de partage en ligne et dans le cloud.

Dans un premier temps, peuvent être mises à jour les politiques internes de sécurité, en concertation avec la DSI, pour minimiser les risques et défi nir les nouveaux outils. Concernant les solutions de stockage, partage et travail en ligne, le cadre contractuel avec le prestataire est crucial et il convient d'être particulièrement attentif aux essentiels que sont la sécurité et la propriété des données ou encore la réversibilité et la responsabilité.

Conformément aux choix stratégiques opérés, la charte informatique de l'entreprise, le livret et guide associés pourront être mis à jour. Les salariés pourront ainsi être sensibilisés à la dangerosité des périphériques USB et informés des nouvelles règles, restrictions d'usage ou interdiction des clés USB, ou encore de la connexion d'autres appareils tels que les smartphones.

Katharina Berbett, « Faille de sécurité de l'USB : quel impact pour l'entreprise ? » , Stratégie internet, n°185, Septembre 2014

Filtrage des flux HTTPS : Droit ou obligation ?

 L'Agence nationale de la sécurité des systèmes d'information (Anssi) vient du publier une recommandation déterminante pour tous ceux qui s'interrogent sur le droit ou non de filtrer les flux https.

Mais au delà de l'intérêt que l'on peut porter à cette recommandations sur son aspect technique on remarquera qu'elle comporte une annexe juridique déterminante

pour tous ceux qui se posent la question de savoir si cette pratique est légale ou non.

L'annexe juridique traite du délicat problème du filtrage flux entrants et sortants depuis les postes de travail fixes et nomades des salariés ou agents d'une entreprise ou d'une entité publique.

Impact. L'Anssi justifie cette démarche tout en rappelant que cette pratique n'est pas sans risque et doit être mise en œuvre avec discernement, dans le respect des obligations légales et singulièrement du droit des données personnelles et du respect de la vie privée des salariés ou agents publics.

L'Anssi légitime et il faut l'en féliciter, le filtrage des flux https au regard de la responsabilité particulière qui pèse sur l'employeur d'une part (article 1384 du code civil), la nécessaire protection de ses intérêts (données, secrets,..) ou encore l'obligation de lutter contre le téléchargement illégal.

Nombreuses sont les entreprises ou les acteurs publics qui aujourd'hui pratiquent un tel filtrage mais qui, faute de cadre juridique, ne rendent pas cette pratique « officielle ». Or les jurisprudences les plus récentes de la Cour de cassation rappellent que tous les outils de cybersurveillance déployé sans respecter les règles essentielles (informations des personnels et déclaration Cnil s'il y a lieu) sont inopposables aux collaborateurs de l'entreprise.

Pour d'autres, la majorité sans doute, ce type de filtrage n'a pas été déployé faute de règles l'autorisant clairement.

Actions. Tout en légitimant l'usage de ce type d'outils, l'Anssi rappelle quelques règles simples :

- Le principe de proportionnalité. Il faut en effet s'assurer du besoin et ne pas filtrer tout et n'importe quoi, par principe … Une analyse d'opportunité amont s'avère donc nécessaire ;
- Le principe de transparence et l'information préalable nécessaire des collaborateurs de l'entreprise – il convient ici de modifier la charte des systèmes d'information en conséquence ;
- La nécessité de prévoir des mécanismes de protection de la vie privée résiduelle des salariés ou des agents ;
- La nécessité de responsabiliser les administrateurs de ce type d'outil. L'Anssi rappelle ici l'importance de disposer d'une charte administrateur ;
- Le respect des obligations issues de la loi informatique et libertés et donc l'obligation de satisfaire a minima aux démarches préalables et de satisfaire au légitime droit d'accès du salarié ou de l'agent public.

Question. Depuis la publication de cette recommandation, la question n'est plus désormais de savoir s'il est légal ou non de déployer une solution de filtrage protocolaire, mais de s'interroger sur les dangers de ne pas le faire.

Il s'agit donc aujourd'hui de savoir si un tel filtrage est un droit ou s'il est devenu une obligation …

Polyanna Bigle

Signature électronique en Europe : nouvelle étape

Signature électronique – L'adoption définitive le 23 juillet 2014 du nouveau règlement eIDAS (electronic identification and trust services), sur l'identification électronique et les services de confiance pour les transactions électroniques marque une nouvelle étape pour la signature électronique en Europe (1).

L'objectif du règlement consiste à « susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur » d'ici 2016. A cette fin, il abroge à la directive 1999/93/CE au 1er juillet 2016 et crée un cadre harmonisé pour différents objets de transaction électronique.

A titre principal, le règlement consacre le marché européen de la signature électronique dans le secteur public et les relations avec les administrés, ainsi que le principe de reconnaissance mutuelle des moyens d'identification électronique délivrés par les Etats membres, tout en exigeant un haut niveau de sécurité pour l'ensemble des méthodes utilisées.

Le règlement reconnaît des notions quasi-inconnues de la législation française, comme l'identification électronique, le document électronique et le cachet électronique (« signature » d'une personne morale déjà reconnu par le référentiel RGS) et la signature électronique qualifiée, proche de la signature dite « présumée fiable » existant en droit français.

Les entreprises, les administrations et les autres organisations telles que les associations vont désormais pouvoir valablement apposer un cachet en leur nom des documents qui seront recevables comme preuve en justice d'origine.

Le règlement prévoit également un statut et des obligations pour les prestataires de services de confiance (PSCE). Une liste des PSCE sera instaurée afin de permettre une reconnaissance mutuelle entre Etats membres.

Si le texte entre en vigueur le 17 septembre prochain, de nombreuses dispositions ne sont applicables qu'à partir du 1er juillet 2016.

La Commission Européenne sera en charge d'édicter des normes et des spécifications pour les différents objets traités par le règlement

Si le Règlement Européen est d'application directe en droit français voué à être modifié, attendons la publication des textes d'application européens et des normes de la Commission.

Par ailleurs, le règlement est à combiner avec le nouveau RGS V2.0 et les

spécifications techniques eIDAS édictées par l'Anssi et son homologue allemand.

Dans le cadre d'un projet de dématérialisation, une legal opinion de conformité européenne et française des solutions de signature électronique serait conseillée.

Polyanna Bigle
Lexing Droit Sécurité des systèmes d'information

(1) Règlement européen n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014.

La future norme ISO 18788 et son impact sur la sécurité privée

La France participe à la rédaction du projet d'une norme ISO qui définira des critères de qualification d'un système de gestion des opérations de sécurité, par la commission de normalisation X51D de l'Afnor « Organisation des services de sécurité et de défense privé ».

Cette commission est le miroir national du comité de projet international ISO/PC 284, dont le domaine des travaux de normalisation concerne « le système de management de la qualité des opérations menées par les entreprises de sécurité privée – Exigences et recommandations ».

La future norme ISO s'adressera aux sociétés de sécurité et de défense privées terrestres, ainsi qu'aux organisations mettant en œuvre un service de sécurité interne pour la surveillance d'infrastructures sensibles et aux pouvoirs publics pour la protection des intérêts français à l'étranger et les cabinets d'audits pour l'évaluation de la conformité. Elle permettra aux utilisateurs d'évaluer leur prestataire de sécurité (interne ou externe), notamment sur la préparation des moyens humains et matériels mis en œuvre pour assurer la mission.

L'Asis, une association de professionnels de la sécurité, qui regroupe 38 000 membres dans le monde, a mis en place une première norme validée par l'Ansi (l'équivalent français de l'Afnor) pour encadrer les activités des sociétés de sécurité (Private Security Company ou Private Security Service Providers).

Ce projet de norme, soumis à l'Iso, est basé sur une norme élaborée par l'Ansi (American National Standards Institute), sur un standard américain du consortium Asis PSC.1 – 2012 « Management standard for quality of private security company operations », elle-même fondée sur l'Icoc (le code de conduite international). Cette norme est déjà applicable avec le Département de la défense (DoD) aux Etats-Unis. Cette norme US est reconnue au Royaume-Uni et en République Tchèque.

L'Ansi, a déjà soumis à l'Iso sa deuxième norme nationale. Destinée aux auditeurs, elle décrit une procédure visant à évaluer la conformité de l'entreprise de sécurité privée aux critères de la norme nationale PSC.1.

Les standards américains Asis PSC.1 et 2, sur lesquels est fondée la future norme ISO, ont été élaborés pour répondre aux capacités des firmes américaines et aux besoins des clients des sociétés américaines. Une fois transcrit en norme Iso, cette future norme favorisera néanmoins les sociétés de défense américaines. L'avantage résultant de l'évaluation de la conformité à cette norme de management, la certification, permettra aux entreprises de services de sécurité et de défense (ESSD) françaises de démontrer aisément que les exigences de la norme sont respectées.

Didier Gazagne
Lexing Droit Intelligence économique

Projet de norme ISO 18788 Management system for quality of private security company (PSC) operations – Requirements with guidance, Voir Afnor.org, actualité du 04-08-2014.

Signaux compromettants : comment protéger les informations ?

 **Signaux compromettants.** L'augmentation de l'utilisation des périphériques et de technologies de communication sans fil induit de nouvelles menaces qu'il convient de prendre en compte pour assurer la confidentialité, l'intégrité, l'authenticité et la disponibilité des informations traitées.

En effet, tout matériel ou système, qui traite ou transmet des informations, sous forme électrique, produit des perturbations électromagnétiques. Ces perturbations, qualifiées de signaux parasites, sont provoquées par les variations du régime électrique établi dans les différents circuits qui composent le matériel considéré durant son fonctionnement.

Certains parasites peuvent être représentatifs des informations traitées. Leur interception et leur exploitation peuvent permettre de reconstituer les informations.

Menace Tempest. C'est la menace constituée par l'interception et l'exploitation des signaux compromettants, en vue de reconstituer les informations traitées. Il s'agit de la menace que font peser les signaux compromettants sur la confidentialité des informations.

Autorité nationale Tempest. L'autorité nationale Tempest est l'autorité qui fixe

les règles applicables en matière de Tempest. Elle veille également au respect et à l'application de la réglementation dans le domaine Tempest. L'Anssi est l'autorité nationale Tempest.

Instruction interministérielle 300. L'instruction s'applique aux systèmes d'information qui font l'objet d'une classification de défense au sens de l'instruction générale interministérielle [IGI 1300] et notamment du titre V concernant les mesures de sécurité relatives aux systèmes d'information.

Les dispositions de l'instruction ont valeur de recommandation pour les systèmes d'information traitant des informations sensibles (en particulier de niveau diffusion restreinte) non classifiées de défense.

En outre, un ensemble de règles techniques qui complètent l'instruction décrivent de façon plus détaillée les différentes mesures de sécurité à mettre en œuvre pour les systèmes classifiés de défense, afin d'interdire la compromission de l'information par l'émission de signaux compromettants.

Se protéger contre la menace Tempest implique une prise en compte globale et continue dans le cycle de vie des systèmes manipulant des informations classifiées. Les dispositions de la présente instruction doivent faire l'objet de clauses particulières dans les marchés et contrats soumis aux dispositions de l'instruction générale interministérielle n°1300 [IGI 1300] qui entraînent la mise en œuvre de systèmes d'information faisant l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées.

Didier Gazagne
Lexing Droit Cybersécurité et cyberdéfense

Piratage téléphonique et responsabilité du prestataire

Piratage téléphonique – Un prestataire de maintenance est condamné pour défaut d'information et d'alerte dans une affaire de piratage de ligne téléphonique.

En juin 2008, une société souscrit des contrats d'adhésion, de location et de maintenance pour la fourniture d'un accès au réseau téléphonique auprès d'un installateur et de sa filiale de maintenance pour une durée de 5 ans.

Informée en janvier 2012 du caractère anormalement élevé de ses consommations téléphoniques -notamment à destination du Timor Oriental- et d'un possible

piratage de sa ligne, la société contacte son installateur privé pour faire changer les codes d'accès sur le matériel téléphonique afin de sécuriser l'installation et « d'enrayer le processus de piratage ».

Le piratage ayant été endigué, elle s'oppose au paiement des factures relatives aux appels passés au Timor Oriental, ce qui engendre une mise en demeure de payer la somme de 21 391, 78 euros.

En avril 2012, la société cliente assigne l'installateur afin d'annuler les factures contestées et d'ordonner la poursuite des contrats devant le Tribunal de commerce de Nanterre. Le tribunal l'a déboute de ses demandes et l'a condamne à payer la somme de 21 391,78 euros, en estimant que l'installateur n'est pas responsable de la maintenance de la ligne téléphonique mais uniquement de son installation et donc ne peut voir sa responsabilité engagée. La société fait appel devant la Cour d'appel de Versailles.

Cette dernière infirme le jugement tout en confirmant la non-responsabilité de l'installateur. En effet, bien que les appels litigieux ne lui sont pas imputables, aucune clause du contrat ne permet à la société cliente de se dégager de ses obligations de payer les factures sauf responsabilité du fournisseur d'accès. En effet, il n'a qu'une obligation de bon acheminement des appels et non une obligation de contrôle de la consommation téléphonique de son client.

En revanche, sur la responsabilité de la société de maintenance, la décision de la cour d'appel diffère de celle du tribunal de commerce. En effet, elle constate que seul le choix d'un mot de passe confidentiel et fréquemment changé est de nature à garantir la sécurisation de l'installation téléphonique de la société cliente. Or, il résulte des pièces du dossier que le mot de passe initial configuré par défaut (0000) n'a jamais été changé.

La cour d'appel en déduit que l'installation n'a jamais été valablement sécurisée, faute de mot de passe personnalisé et régulièrement modifié. Elle retient que la société de maintenance est tenue par les termes du contrat de maintenance : sa responsabilité peut donc être engagée si depuis la conclusion du contrat, elle a manqué à ses obligations d'information et de conseil.

Si elle a accompli la mission de réparation qui lui incombait, elle n'a en revanche pas accompli les missions d'information et de conseil quant aux évolutions techniques en matière de télécommunications pouvant intéresser l'exercice de son activité et de « visite préventive annuelle », comme il était prévu dans le contrat de maintenance.

C'est donc à bon droit que la société cliente se plaint de n'avoir pas été suffisamment informée pour lui permettre de mieux sécuriser sa ligne. Elle est donc fondée à rechercher la responsabilité de la société de maintenance qui a manqué à ses obligations contractuelles en ne lui donnant pas les moyens d'éviter le piratage dont elle a été victime. Le prestataire de maintenance est condamné à payer la somme de 18 000 euros à titre de dommages et intérêts et de 2 000 euros au titre de l'article 700 du CPC.

Virginie Bensoussan-Brulé
Lexing Droit pénal numérique

(1) CA Versailles 12e ch 25-03-2014, n°1207079 SARL Les Films de la Croisade c SAS Nerim.

La sécurité de l'internet des objets au cœur de son développement

 L'internet des objets, c'est « l'objet le plus usuel (pour ne pas dire « bête») qui deviendrait intelligent… l'objet le plus anodin sera alors en mesure de communiquer avec l'environnement qui les entoure ».

La définition retenue par des précurseurs de l'internet des objets (« IdO ») est « un réseau de réseaux qui permet, via des systèmes d'identification électronique normalisées et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant» (1).

L'internet des objets regroupe de manière large les objets reliés entre eux « machine to machine » (« MtoM ») et des objets reliés à des systèmes d'information passant par internet.

Partant du constat qu'internet n'est pas un « lieu » sécurisé, la sécurité de l'IdO est au cœur de sa mise en place et prendra une importance grandissante.

Trois problématiques de sécurité se dégagent déjà dans l'IdO :

- la sécurisation de l'identité des objets dans IdO ainsi que des données du monde physique récupérées, stockées et transférées ;
- la sécurisation des transmissions d'ordre d'action, nécessitant des garanties techniques et contractuelles ;
- les moyens de lutte contre une cybercriminalité des IdO.

Cette ouverture du monde physique des objets à l'internet avec ou sans l'action de la main de l'homme nécessite en effet que les aspects de sécurité technique et juridique soient bien maîtrisés. Les « cybercrimes » vont peut-être changer de mode de déploiement, mais certainement pas d'objectifs : soustraction frauduleuse d'argent ou de biens, usurpation d'identité, abus de confiance et dol, espionnage industriel, etc…

Sécurité de l'identité d'un objet. La sécurisation de l'identité des objets dans l'IdO pourrait sembler purement technique : cadre technique sécurisé avec systèmes d'authentification élevés, moyens de cryptologie, création de fédération d'identité d'objets, etc…

Cependant la sécurité de l'identité d'un objet est aussi juridique. Si tant est qu'un objet dispose d'une « identité » juridique, sans rentrer dans le débat, derrière l'identité d'un objet, c'est l'identité de son « maître » ou plutôt de son « propriétaire » qu'il convient de protéger.

Ainsi le système d'identification de l'objet devra sans doute répondre, dans une mesure adaptée, au cadre légal de la protection des données à caractère personnel sur l'identification, la traçabilité et la surveillance.

L'utilisation des prestataires de services de confiance deviendra un impératif nécessaire, d'autant qu'ils sont soumis à un cadre légal déjà défini. Rappelons qu'au sens de l'Ordonnance du 8 décembre 2005, son rôle consiste à offrir « des services tendant à la mise en oeuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique » (2). La course aux prestataires de services de confiance qualifiés est ainsi ouverte vu les potentiels du marché de l'IdO.

La sécurisation des ordres de transmission. Dans les exemples de la vie quotidienne, l'IdO, c'est le réfrigérateur qui commande au supermarché les denrées alimentaires manquantes selon un contrat conclu entre le supermarché et le propriétaire.

Là encore, outre les aspects de paramétrage technique et de choix d'un réseau sécurisé (réseau privé virtuel) ou internet « world wide web », de choix d'un administrateur externe ou interne, des problématiques de garantie contractuelles émergent.

D'une part les normes et référentiels de sécurité ainsi que les guides des bonnes pratiques de sécurité comme par exemple ceux publiés par l'Agence Nationale pour la Sécurité des Systèmes d'Information (Anssi), vont devenir les références essentielles dans les contrats d'IdO, comme gage de la sécurité

D'autre part, il parait essentiel que les clause de sécurité des contrats d'IdO soient rédigées avec soin, développent les plans de mise en œuvre de la sécurité et de détection des failles et intrusions, etc…, et surtout les garanties associées adéquates pour la protection du consommateur, de sa famille, ou du professionnel qui l'utilise pour son entreprise.

L'IdO ne peut se développer que dans un cadre de confiance fort entre ses acteurs « humains ».

Au niveau contractuel, un des différents contractuels principal qui pourra découler d'un défaut de sécurité, sera la contestation de l'ordre de transmission et donc la preuve de la commande : le propriétaire de l'objet relié à internet contestera l'ordre de transmission et par là même la commande. Les conventions de preuve auront tout leur rôle à jouer.

La lutte contre des « cybercrimes » de l'IdO. Si bien entendu l'arsenal des délits et crimes de droit commun demeurent applicables à l'IdO comme le vol, l'abus de confiance, la contrefaçon, ou même l'atteinte à l'intégrité d'une personne tout en priant pour que le scénario d'IdO tueur ne reste que pure fiction.

En droit de l'informatique, le cadre légal est et semble demeurer celui de la loi dite Godfrain adoptée en 1988 codifiée aux articles 323-1 et suivants du Code pénal réprimant les « atteintes aux systèmes de traitement automatisés de données ». Voici pour mémoire ces textes pérennes :

- « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans

d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende. Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende. »

- « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende. »
- « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende. »

Derrière l'objet, se trouve nécessairement l'homme et la responsabilité qu'il devra supporter. Mais la problématique judiciaire sera là encore la question des preuves et de la traçabilité des cybercriminels qui décideront de s'attaquer aux IdO.

On n'oubliera pas l'existence de l'article 34 bis sur les violations de données à caractère personnels qui aura vocation à s'appliquer à l'IdO et faisant peser des risques pénaux sur les fournisseurs de communication électronique en cas de défaillance de sécurité de leur réseau.

Enfin, si le sport favori des nouveaux cybercriminels est de faire passer un objet relié au réseau par un autre objet, les délits d'usurpation d'identité des articles 226-4-1 et 434-23 du Code pénal pourront servir l'arsenal judiciaire. La problématique sera alors de savoir dans quelle mesure l'identité d'un objet usurpée se considérée comme l'identité de son propriétaire.

En conclusion, l'IdO doit conduire dès maintenant à revoir les questions de sécurité tant au niveau organisationnel, qu'au niveau contractuel, par une « sécurité by design ». Ainsi, les analyses de risques juridico-techniques des solutions proposées en amont et de leurs mises en œuvre en aval sont plus que nécessaires.

Polyanna Bigle
Lexing Droit Sécurité des systèmes d'information

(1) « L'Internet des objets. Quels enjeux pour l'Europe ? », Ed. Maison des sciences de l'Homme, Paris, 2009 – Françoise MassitFolléa – Pierre-Jean Benghozi et Sylvain Bureau.
(2) Ord. n° 2005-1516 du 8 12 2005.

Serious Game et sécurité des systèmes d'information

Avec « Keep an Eye », le Serious Game étend l'arsenal à la disposition des entreprises pour garantir la sécurité de leurs systèmes d'information et prouve ainsi une nouvelle fois la grande plasticité d'usage qui est l'origine de son succès.

Né de l'initiative du Cigref sur la base des recommandations de l'ANSII, « Keep an Eye » est un Serious Game (Jeu Sérieux) ayant pour double objectifs de sensibiliser les employés à la sécurité des systèmes d'information et de répandre chez ces derniers la culture du risque dans l'entreprise (1).

Pour y parvenir, « Keep an Eye » propose de former les joueurs à la gestion des risques par le biais d'une simulation. Le joueur se voit ainsi proposer de devenir l'« ange gardien » d'un homme d'affaires en mission avec pour objectif de garantir la sécurité de ses données.

La protection des systèmes d'information est une problématique à laquelle toutes les entreprises sont aujourd'hui confrontées et qui ne cesse de prendre de l'ampleur.

Si la protection des systèmes d'information passe nécessairement par la mise en œuvre de moyens techniques et organisationnels adaptés, il est également crucial pour les entreprises de ne pas sous-estimer le facteur humain.

Chaque employé ayant un accès au système d'information de l'entreprise, l'humain représente en effet un risque majeur pour l'intégrité du système et des informations sensibles qu'il contient.

En facilitant la diffusion des bonnes pratiques d'utilisation des systèmes d'information parmi les employés, le Serious Game semble être l'outil idéal pour se prémunir de ce risque.

Encore faut-il bien évidemment que ces bonnes pratiques d'utilisation aient été définies au préalable au sein de l'entreprise, a minima dans le cadre d'une charte des systèmes d'information.

Benoit de Roquefeuil
Arnaud Marc
Lexing Contentieux informatique

(1) Cf. Le fil numérique du Cigref, N° 8 Juin 2014.

Signature électronique : conférence et atelier Documation

 **Signature électronique –** Polyanna Bigle intervient dans le cadre d'une conférence initiée par Documation, portant sur les principes techniques, la valeur légale et les bénéfices de la signature électronique.

Elle participe également à un atelier organisé sur cette thématique, ce qui lui permet de faire part de son expertise concernant les solutions de signature manuscrite électroniques, le cabinet ayant réalisé la première legal opinion sur cette thématique.

Avec internet apparaissent de nouvelles formes de signatures qui se propagent dans les usages quotidiens. Des signatures effectuées sur tablettes électroniques, par courriel ou par d'autres moyens (QR code-code barre 2D), aux signatures à la volée ou éphémères proposées par les plateformes de signature en ligne, la signature électronique entre dans les mœurs.

Autrefois réservée à des applications professionnelles, elle se déploie dans le grand public à une vitesse impressionnante avec l'e-commerce. De nombreuses plateformes proposent aux entreprises de faire signer électroniquement tous types de documents à leurs correspondants professionnels ou particuliers et d'ajouter un bouton « Signer » à leur site Internet, de la même façon qu'un service de paiement en ligne. Il s'agit la plupart du temps d'un code à usage unique envoyé par SMS sur le téléphone mobile de l'internaute afin de lui permettre d'accepter le document qu'il visualise. Ces solutions de contractualisation numérique font partie d'une stratégie multicanal BtoB et BtoC qui permet d'accélérer le développement commercial, en améliorant le taux de transformation.

Le renouveau de la signature électronique, constaté avec le développement des nouveaux moyens de communication, s'accompagne d'une évolution du cadre légal, la loi du 13 mars 2000 adaptant le droit de la preuve aux technologies de l'information et relative à la signature électronique ayant révolutionné notre Code civil.

Par principe, la signature électronique pourra s'apposer sur quasiment tous les types d'actes. Les conditions sont simples mais techniques : la nécessité de pouvoir identifier la personne dont il émane et une garantie d'intégrité dans la création et la conservation de l'acte signé. Par exception, certains actes ne pourront pas être établis électroniquement et par là-même ne pourront être signés électroniquement.

La mise en oeuvre d'un processus de signature électronique ne doit pas se faire à l'aveuglette : outre le choix d'un bon prestataire, le juriste de l'organisme devra être intégré à l'équipe projet. En effet, une analyse juridique en amont

est essentielle.

Une proposition de règlement européen en voie d'adoption devrait bénéficier aux particuliers comme aux entreprises. Le règlement proposé leur permettra en effet « d'utiliser le système national d'identification électronique de leur pays pour accéder aux services publics en ligne dans d'autres pays de l'Union européenne où l'identification électronique est disponible ».

Vidéo de l'intervention de Polyanna Bigle, programme de la conférence et programme de l'Atelier du 27 mars 2014.

Coffre-fort numérique : création d'un label Cnil

 **Coffre-fort numérique** – La Cnil adopte pour la première fois un référentiel permettant la délivrance de labels en matière de services de coffre-fort numérique (1), synonyme ici de « coffre-fort électronique » dans le prolongement de ses recommandations de 2013 (2).

Ce référentiel contraignant concerne « les offres proposées à des particuliers de services de stockage, dématérialisé et sécurisé, de données, et dont l'objet est de conserver des documents sur un support informatique ». Ces offres se distinguent des espaces de stockage en ce que « les données conservées incluant les documents stockés et leurs métadonnées ne sont accessibles qu'au seul titulaire du coffre et, le cas échéant, aux personnes physiques que le titulaire a spécifiquement habilitées à cet effet ».

Cette définition renvoie directement à la définition par la Cnil des services dits de coffre-fort numérique ou électronique.

Ce label est réservé aux candidats au label à la fois opérateurs techniques du service et fournisseurs de ce service auprès des particuliers qui démontrent, par des justifications argumentées et des éléments de preuves, qu'ils satisfont aux conditions posées par le référentiel.

Dans le cas où ces fonctions sont dévolues à deux personnes morales distinctes, la demande de label devra être formulée conjointement par l'opérateur et le fournisseur, afin de justifier de la conformité au référentiel.

La délivrance du label est subordonnée à la démonstration, par le candidat, du respect de 22 exigences cumulatives portant sur :

- la démarche de conformité mise en œuvre par le fournisseur du service « qui doit, pour l'ensemble des traitements qu'il met en œuvre, veiller à la

protection des données personnelles au-delà du seul service objet de la demande de label » ;
- et sur « la protection des données du service de coffre-fort numérique, objet de la demande de label, reprenant : les données traitées, l'accès aux données, la conservation des données, l'information des personnes, la gestion des risques et les mécanismes cryptographiques ».

La délivrance du label par la Cnil impose ainsi notamment la démonstration par le candidat que le service satisfait à des obligations relatives à la gestion des risques, à la conformité et aux mécanismes cryptographiques intégrés dans le service de coffre-fort numérique.

Dans la mesure où la labellisation Cnil constitue un marqueur fort permettant au consommateur de s'orienter vers les services les plus respectueux des données personnelles, il revient aux prestataires offrant des services de coffre-fort numérique de les auditer afin de démontrer la conformité de leur service aux exigences du label ou de déterminer les moyens techniques nécessaires au respect de ce standard.

Selon l'article 2.5 de l'annexe de la délibération, cette analyse de conformité devra en outre être renouvelée tous les trois ans, au même titre que l'étude des menaces et l'audit de l'effectivité et de l'efficacité des mesures choisies.

Polyanna Bigle
Jean-Baptiste Gevart
Lexing Droit Sécurité des systèmes d'information

(1) Délib. 2014-017 du 23-1-2014.
(2) Délib. 2013-270 du 19-9-2013.

Comment mettre en œuvre la mobilité en entreprise ?

Comment mettre en œuvre la mobilité en entreprise ? du 12 mars 2014 – Emmanuel Walle a animé un petit-déjeuner débat consacré à la mobilité en entreprise. Xavier de Mazenod, spécialiste de la communication d'influence, des réseaux sociaux et du télétravail et consultant associé de la société Adverbe était également présent.

Les technologies numériques rendent l'entreprise plus mobile, plus efficace et plus productive en créant de nouvelles façons de travailler ensemble. Le Premier Ministre a mis cette priorité dans sa feuille de route le 28 février 2013, à l'occasion d'un séminaire gouvernemental dédié au numérique pour une économie plus compétitive.

Les technologies numériques offrent également de nouveaux services de mobilité que la gestion des ressources humaines doit intégrer. Pour la DRH, les enjeux sont organisationnels et juridiques (comptabilisation du temps de travail, contrôle d'activité, etc.).

A titre d'exemple, il existe aujourd'hui de nombreuses « applis » qui permettent aux collaborateurs nomades d'enregistrer et de transmettre depuis leur Smartphone ou tablette, des éléments de gestion (notes de frais, déclarations de congés, etc.). Elles soulèvent de nombreuses questions sur la sécurité du système d'information et la gestion des RH.

Ce petit-déjeuner a été l'occasion d'examiner les questions suivantes :

- Quels est l'impact des innovations technologiques sur la mobilité du travail ?
- Quelles sont les nouvelles questions qui se posent à la DRH ?
- Comment gérer et contrôler l'aménagement du temps de travail « nomade » ? (forfaits jour, annuel, etc.)
- Quels sont les risques en cas de contentieux du travail ? (preuve du temps de travail effectif, paiement des heures supplémentaires, accident du travail, etc.)
- Quant peut-il y avoir requalification du contrat de travail ?

Le petit-déjeuner a eut lieu dans nos locaux, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris.

Pacte Défense Cyber : vers la création d'un pôle d'excellence

Pacte Défense Cyber – La cyberdéfense a été élevée par le Livre Blanc sur la Défense et la Sécurité nationale (1) et dans la Loi de programmation militaire 2014-2019 au rang de priorité nationale. Le Pacte Défense Cyber, présenté par le Ministère de la Défense le 7 février dernier, dresse tous les aspects de la cyberdéfense : les mesures propres au Ministère de la Défense bien entendu, mais aussi les mesures destinées à créer, développer ou soutenir des initiatives de collectivités locales, de grands groupes ou des PME du secteur défense. Il a d'ailleurs été élaboré en prenant pour modèle le Pacte Défense PME.

Les enjeux principaux du Pacte Défense Cyber sont notamment l'élévation du niveau de préparation des forces et des emprises du Ministère de la Défense face aux menaces, le développement d'une base industrielle et technologique de cyberdéfense, de stimuler la recherche et la formation par la création d'un pôle

d’excellence cyberdéfense en Bretagne, de poursuivre avec le pôle d’excellence, la mise en place d’un réseau de simulation et enfin de contribuer au renforcement de la communauté nationale de défense.

Le Pacte Défense Cyber s’articule autour de 6 axes comprenant plus de 50 actions stratégiques.

Axe 1 : Cet axe a pour objectif de durcir le niveau de sécurité et les moyens de défense afin d’obtenir une plus grande résilience des systèmes d’information de l’Etat. Cet axe se traduira par 16 actions portant notamment sur le renforcement du niveau de cyberdéfense du Ministère de la défense et l’utilisation de logiciels ou applications développées ou maîtrisées au plan national, la création, le maintien et l’utilisation d’outils de cybersécurité de niveau élevé ainsi que le développement et le déploiement de capacité avancées de détection et d’intervention.

Axe 2 : Cet axe vise à préparer l’avenir par l’intensification de l’effort de recherche technique et académique. Il se traduit par 10 actions stratégiques.

Axe 3 : L’enjeu de cet axe est le renforcement des ressources humaines dédiées à la cyberdéfense et à la construction de parcours professionnels dédiés.

Axe 4 : Cet axe vise le développement du Pôle d’excellence en cyberdéfense en Bretagne et de la communauté nationale de Cyberdéfense. En particulier, l’une des actions stratégiques de cet axe poursuit l’objectif de renforcer l’intégration de la cyberdéfense dans la préparation opérationnelles des forces, sous la coordination du CALID Bretagne et avec l’expertise de la DGA-MI.

Axe 5 : Cet axe consiste à bâtir un réseau de partenaires, en Europe et au sein de l’Alliance Atlantique. L’une des actions de cet axe consiste dans la constitution d’une plate-forme distribuée de formation et d’entraînement pour former et entraîner à la cyberdéfense mais aussi à la gestion de crise cybernétique.

Axe 6 : L’enjeu de cet axe est de favoriser l’émergence d’une communauté nationale de cyberdéfense et en particulier au développement de la réserve citoyenne de cyberdéfense.

Didier Gazagne
Lexing Droit Risques technologiques

Le renouveau de la signature électronique

 **Petit-déjeuner Le renouveau de la signature électronique du 29 janvier 2014 –** Polyanna Bigle a animé, avec Dimitri Mouton (société Demaeter), un petit-déjeuner débat dédié au renouveau de la signature électronique. Avec internet apparaissent de nouvelles formes de signatures qui se propagent dans les usages quotidiens.

Des signatures effectuées sur tablettes électroniques, par courriel ou par d'autres moyens (QR code-code barre 2D), aux signatures à la volée ou éphémères proposées par les plateformes de signature en ligne, la signature électronique entre dans les mœurs.

Autrefois réservée à des applications professionnelles, elle se déploie dans le grand public à une vitesse impressionnante avec l'e-commerce. De nombreuses plateformes proposent aux entreprises de faire signer électroniquement tous types de documents à leurs correspondants professionnels ou particuliers et d'ajouter un bouton « Signer » à leur site Internet, de la même façon qu'un service de paiement en ligne. Il s'agit la plupart du temps d'un code à usage unique envoyé par SMS sur le téléphone mobile de l'internaute afin de lui permettre d'accepter le document qu'il visualise. Ces solutions de contractualisation numérique font partie d'une stratégie multicanal BtoB et BtoC qui permet d'accélérer le développement commercial, en améliorant le taux de transformation.

Ce petit-déjeuner a été l'occasion d'examiner les questions suivantes :

- Quelle est la valeur juridique des signatures à la volée ou sur tablette ?
- Quelle est la qualité des preuves électroniques ?
- Comment maîtriser les risques juridiques ?
- Comment rédiger une convention sur la preuve ?
- Qu'est-ce qu'un dossier de preuve ou un chemin de preuve ?
- Qu'y a-t-il concrètement derrière ces différentes formes de signature électronique?

Le petit-déjeuner a eut lieu dans nos locaux, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris.

Sécurité des systèmes d'information de santé

 Un guide de la sécurité des Systèmes d'Information de santé des

établissements de santé a été publié par la Direction Générale de l'Offre de Soins (DGOS) a publié, courant du mois de novembre 2013 (1).

La confidentialité et l'intégrité des données sensibles, ainsi que la continuité des soins doivent en effet constituer les préoccupations majeures des établissements de santé en termes de sécurité du SI.

Le guide s'intègre à la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) dont le corpus documentaire continue donc à s'étoffer. La PGSSI-S, déjà constituée de quelques documents pivots (principes fondateurs, référentiels thématiques de sécurité, guides pratiques et juridiques) est en effet en cours d'élaboration.

Le guide de la DGOS a cependant vocation à constituer un outil autonome et pratique qui décrit la démarche de sécurité des systèmes d'information de santé à mettre en œuvre aux établissements de santé et contient des recommandations pratiques. Il participe à la fourniture, aux Directions des établissements de santé (DG, Président de la Commission Médicale d'Etablissement, Directeur des soins, DSI, etc.), tant publics que privés, des clés pratiques en vue de la sécurité des SI et de l'initialisation de démarches pérennes.

Les points clés de la démarche de sécurité des systèmes d'information de santé s'articulent autour des 10 fiches pratiques suivantes :

– les enjeux de la sécurité de l'information pour l'établissement de santé. Les risques internes ou externes qui pèsent sur l'établissement sont, à cette occasion, mis en évidence ;
– la maîtrise de la sécurité du système d'information. L'intégrité, la confidentialité des informations médicales ainsi que la continuité des soins sont placées au cœur des objectifs de l'établissement ;
– la définition de la sécurité du système d'information dans les établissements de santé. La mise en œuvre d'un plan de sauvegarde ainsi que d'un plan de reprise et de continuité de l'activité sont présentés comme incontournable ;
– la direction : acteur important de la démarche de sécurité ;
– les pré-requis : un diagnostic et une gouvernance sécurité ;
– la sécurité avant d'autres projets : le bon arbitrage ;
– les facteurs clés de succès de la démarche ;
– la communication : un levier essentiel ;
– la documentation sécurité : un minimum, constitué notamment d'une cartographie des risques, d'une politique de sécurité du système d'information et d'une charte d'utilisation du système d'information et de télécommunication, est nécessaire ;
– les coûts de la sécurité.

Marguerite Brac de La Perrière
Lexing Droit Santé numérique

(1) Guide pour les Directeurs d'établissement de santé, DGOS, nov. 2013.

La loi de programmation militaire : un processus plus transparent

 Interviewé par Metronews sur le projet de loi de programmation militaire, Alain Bensoussan répond aux questions de Jean-Sébastrien Zanchi. Pour lui, la loi amène plus de clarté à des pratiques déjà existantes. Il estime que « cette loi est un véritable mieux par rapport à la situation actuelle. Le processus est bien plus transparent et permet une traçabilité de la surveillance. Le cadre juridique actuel est très complexe, plusieurs textes s'y télescopent, comme le droit des télécoms ou la loi informatique et libertés ».

L'article 20 de la loi de programmation militaire élargit le champ d'accès aux données téléphoniques et informatiques des Français, détenues par les opérateurs télécoms et les hébergeurs. Se faisant, il lève ainsi une incertitude suscitée par la rédaction de l'article L. 34-1-1 du Code des postes et des communications électroniques et de l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique en autorisant expressément les services de police et de gendarmerie chargés de la prévention du terrorisme à accéder en temps réel à des données de connexion mises à jour, ce qui leur permet de géolocaliser un terminal téléphonique ou informatique et de suivre ainsi en temps réel certaines cibles, dans le cadre de la lutte contre le terrorisme.

Pour Alain Bensoussan, l'essentiel est de « trouver un équilibre entre le droit des personnes et la lutte contre le terrorisme ».

La loi a été adoptée le 18 décembre 2013 (JO du 20-12-2013)

Alain Bensoussan pour Metronews, le 12 décembre 2013.

Assises de la sécurité et des systèmes d'information 2013 : lecabinet est présent !

 Alain Bensoussan participe à la 13ème édition des Assises de la sécurité et des systèmes d'information, qui se déroulent au Grimaldi Forum à

Monaco du 2 au 5 octobre 2013. Les Assises de la sécurité sont un événement très attendu par les décideurs des SSII (RSSI, DSI, DI, Risk managers, Correspondant Informatique et libertés) qui peuvent, lors de conférences plénières, de tables-rondes entre experts et d'ateliers thématiques, échanger sur les problématiques majeures de sécurité informatique, tant nationales qu'internationales.

Alain Bensoussan intervient dans le cadre d'une table ronde portant sur le thème « Le DPO : nouvelles missions, nouvelles responsabilités », afin de préciser le rôle, les qualifications et les obligations du correspondant Informatique et libertés (Cil) en regard des dispositions du projet de règlement européen sur la protection des données.

Le DPO (Data Protection Officer) va en effet devenir un acteur incontournable de la conformité relative à la protection des données. Les entreprises doivent ainsi d'ores et déjà connaître les contours des obligations et les challenges qui vont être pris afin d'intégrer ce nouvel acteur. Donner les clés aux entreprises afin de permettre un passage en douceur lors de la promulgation du futur règlement. Les intervenants de ce débat partageront leur expérience et les best practices à implémenter, tels que des relais de DPO ou des procédures.

La signature électronique : l'essayer, c'est l'adopter !

La signature électronique « pour tous », en fort développement, a vocation à se généraliser, non seulement dans la vie des affaires, mais également dans la vie courante. La loi de 2000 adaptant le droit de la preuve aux technologies de l'information et relative à la signature électronique a en effet révolutionné notre Code civil (1). En témoigne la récente décision de la Cour d'appel de Nancy (2) qui a reconnu la validité d'une signature électronique apposée par un particulier sur une autorisation de découvert de 9 000 euros proposée par sa banque. Une autre décision de première instance vient de valider le recours à la signature électronique proposée par un prestataire de services pour saisir la juridiction de proximité (3).

Par principe, la signature électronique pourra s'apposer sur quasiment tous les types d'actes. Les conditions sont simples mais techniques : la nécessité de pouvoir identifier la personne dont il émane et une garantie d'intégrité dans la création et la conservation de l'acte signé. Par exception, certains actes ne pourront pas être établis électroniquement et par là-même ne pourront être signés électroniquement.

La mise en oeuvre d'un processus de signature électronique ne doit pas se faire à l'aveuglette : outre le choix d'un bon prestataire, le juriste de l'organisme devra être intégré à l'équipe projet. En effet, une analyse juridique en amont

est essentielle.

Une proposition de règlement européen en voie d'adoption devrait bénéficier aux particuliers comme aux entreprises. Le règlement proposé leur permettra en effet « d'utiliser le système national d'identification électronique de leur pays pour accéder aux services publics en ligne dans d'autres pays de l'Union européenne où l'identification électronique est disponible » (4).

Polyanna Bigle pour Archimag, juin 2013 (n° 265) et juillet-août 2013 (n° 266)

(1) Loi 2000-230 du 13-3-2000
(2) Lire notre précédent post du 5-6-2013
(3) TI Antibes 7-3-2013 M. B c/ Free Mobile
(4) Commission européenne, Proposition de règlement européen COM(2012) 238 final du 4-6-2012 et Communiqué de presse du 4-6-2012

Télétravail : quelle stratégie juridique adopter ?

 Le cadre juridique instaure désormais un régime plus sécurisé en matière de télétravail « gris ».

Qu'il s'agisse de répondre à des besoins identifiés dans l'entreprise, de satisfaire à un modèle économique nouveau (augmenter l'employabilité des salariés), de s'adjoindre des compétences à forte valeur ajoutée ou encore d'accéder à l'opportunité de purger le télétravail « gris » en l'habillant des dispositions récentes du code du travail, le cadre juridique instaure désormais un régime plus sécurisé.

Le télétravail répondait déjà à un référentiel obligatoire (1), que la codification a généralisé en y ajoutant l'option d'un télétravail en cas de circonstances exceptionnelles.

Le cadrage du télétravail implique un processus de sélection des demandes et, le cas échéant, une démarche d'arbitrage : il n'est pas fait pour tous et demande une autonomie suffisante. Ce type de contrat peut être prévu dès l'embauche ou plus tard sur la base du volontariat et par avenant au contrat de travail, sur sollicitation du salarié ou de l'employeur. Mais l'initiative est loin d'être neutre, car elle a un fort impact sur la prise en compte des coûts.

De manière générale, les aspects santé et sécurité pourront renvoyer à la charte d'utilisation des systèmes d'information et au règlement intérieur. L'accord collectif semble être un facteur clé de succès (gestion des aspects psychosociaux, règles d'indemnisation de l'occupation professionnelle du

domicile, etc.), surtout si l'on y ajoute les dispositions majeures relatives au temps de travail, pour éviter une requalification ou un rappel d'heures supplémentaires.

Emmanuel Walle pour L'Usine nouvelle, le 15 septembre 2013

(1) Accord national interprofessionnel du 19-7-2005 qui transpose l'accord-cadre européen du 16-7-2002, étendu par l'arrêté du 30-5-2006.

Cnil : Procédure en ligne de notification des violations de données

La Cnil a créé sa procédure en ligne de notification des violations de données personnelles le 23 août 2013 (1). Cette procédure, effective depuis le 25 août, fait suite à la publication du règlement européen du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel qui impose aux autorités de protection des données de mettre à disposition des fournisseurs de communications électroniques une procédure de notification des violations de données à caractère personnel.

Pour rappel, l'obligation de notification, qui incombe pour l'heure uniquement aux fournisseurs de communications électroniques, résulte de la ratification de la directive Paquet Telecom, qui a été transposée à l'article 34 bis de la loi Informatique et libertés.

Dès lors, si un fournisseur de communications électroniques constate une violation de données personnelles, il devra utiliser le formulaire téléchargeable sur le site internet de la Cnil, lequel pourra être adressé par la même voie. La Cnil met également à leur disposition un outil d'aide à l'analyse du degré de gravité de la violation de données personnelles.

Cette télé-procédure sera probablement étendue dans un futur proche, dans la mesure où le projet de règlement européen de protection des données à caractère personnel du 25 janvier 2012 prévoit l'extension de l'obligation de notification à tous les responsables de traitement.

Polyanna Bigle
Lexing Droit Sécurité des systèmes d'information
Caroline Macé
Lexing Droit Informatique et libertés contentieux

(1) Cnil, Rubrique Actualité, article du 23-8-2013

L’avenir des ESSD en France : les perspectives juridiques

Alain Bensoussan est intervenu au colloque sur l’avenir des ESSD en France, organisé par le Conseil supérieur de la formation et de la recherche stratégiques (CSFRS), dirigé par Alain Bauer, en partenariat avec le Club des directeurs de sécurité des entreprises (CDSE) présidé par Alain Juillet, qui s’est tenu à l’Ecole militaire, le 28 mai 2013. S’intéressant aux perspectives juridiques, Alain Bensoussan a tracé les grandes lignes des modifications pouvant être envisagées afin de faire évoluer le secteur des ESSD.

L’enjeu, c’est un marché économique stratégique. Le défi c’est l’acceptabilité sociale, on ne peut pas externaliser la souveraineté. L’actualité, c’est la multiplication des zones de conflit sans guerre au sens du droit de la guerre. Le contexte international et géostratégique actuel est en effet caractérisé par la multiplication des crises régionales et des théâtres d’opérations à intérêts stratégiques. Comme il n’y a pas de guerre, il ne peut y avoir de militaires. Ce qui explique le recours croissant à des entreprises de services de sécurité et de défense (ESSD), qualifiées indûment par certains de mercenaires ou de corsaires, termes à bannir parce qu’étant inappropriés.

La situation légale est paradoxale et se situe à la fois dans le vide juridique mais aussi dans le trop plein. Il faut faire évoluer certains éléments de langage. La sécurité ressort de la souveraineté, il est donc nécessaire de recourir aux concepts de protection et de tranquillité, appartenant eux, au domaine du marché privé.

Il faut aussi faire évoluer la situation légale contraignante relative à l’acquisition, au stockage et au transport d’armes, de munitions et d’équipements de sécurité. L’enjeu important c’est évidement le transport et la détention des armes. Il est possible de modifier les textes en matière d’armes, pour un objectif défensif et non offensif. Par ce biais-là, en créant une norme, un label, des certificats et des contrats, la norme du marché sera l’avenir de la loi future.

Voir les actes du Colloque du 28-5-2013.