Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Protection des données et risques juridiques

Un Livre Blanc de Check Point Software

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Sommaire

Préambule 3
I. Contexte 4
II. Ce que dit la Loi… 7
III. Les risques juridiques encourus 10
IV. Bonnes pratiques 13
V. Solutions 15
VI. Références 18

Préambule

L'information est au cœur de l'entreprise. Elle est capitale pour son activité. Avec l'avènement d'Internet, et la multiplication des réseaux et périphériques communicants, les échanges d'informations croissent de façon exponentielle. Depuis quelques années, cette vie numérique s'est organisée autour des différents acteurs de l'entreprise : collaborateurs (également utilisateurs des nouvelles technologies dans leur cadre privé), partenaires, fournisseurs, exploitants… Tous communiquent et partagent des données souvent sensibles. Pour beaucoup d'entre nous, Internet est devenu le « réseau local » de l'entreprise, réseau qui comporte de nombreux dangers pour les données : vols, piratage, détournements, utilisations frauduleuses… Le catalogue des menaces initiées par les cyber-criminels est hélas à la hauteur des profits générés : impressionnant.

L'information est devenue source de convoitise. Et pour cause : un fichier clients, un bilan, des données personnelles ou encore des données relatives à un savoir-faire se monnaient aisément et chers sur le « marché souterrain ». L'entreprise se doit de protéger ses données. Elle y est contrainte par un cadre législatif qui s'est étendu à toute l'Europe.

La Loi «Informatique et Libertés» de 1978 impose que les organismes mettant en œuvre des traitements ou disposant de fichiers de données en garantissent la sécurité. Par sécurité des données, on entend l'ensemble des «précautions utiles, au regard de la nature des données et des risques présentés par le traitement», pour notamment, «empêcher que les données soient déformées, endommagées, ou que des tiers non autorisés y aient accès.» (Art.34 loi IL). Cette sécurité se conçoit pour l'ensemble des processus relatifs à ces données, qu'il s'agisse de leur création, leur utilisation, leur sauvegarde, leur archivage ou leur destruction et concerne leur confidentialité, leur intégrité, leur authenticité et leur disponibilité.

L'objectif de ce Livre Blanc est triple :
- Sensibiliser les entreprises sur l'impérieuse nécessité de protéger ses données.
- Rappeler les principales réglementations en vigueur.
- Indiquer aux dirigeants et responsables de la sécurité les bonnes pratiques à suivre et les solutions à adopter pour renforcer la protection de leur système d'information tout en restant en conformité avec les textes de Lois.

Check Point Software remercie tous ceux qui ont contribué à la réalisation de ce Livre Blanc et plus particulièrement Maître Isabelle Renard (Cabinet Racine), Maître Olivier Iteanu (Cabinet Iteanu) et Olivier Pantaléo (Président de Provadys et de Majj).

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

I. Contexte

Les données constituent le cœur du système d'information de l'entreprise, au centre d'un vaste processus économique. Leur valeur est inestimable. D'elles dépendent son activité, son développement, son ouverture sur le monde. Avec Internet et le développement des réseaux et l'avènement de la « société numérique », les données subissent de multiples traitements facilitant les échanges d'informations, de biens et de services.

Les données sont devenues des denrées précieuses pour tous les acteurs de la vie économique mais aussi pour les cybercriminels qui les exploitent à leur profit. Au cours des deux dernières décennies, les techniques mises en œuvre par les pirates informatiques se sont développées pour exploiter toutes les failles de sécurité qui s'offrent à eux.

Les menaces Web ou « malwares » (virus, vers, chevaux de Troie, phishing, logiciels espions…) sont en constante progression. Entre 2005 et 2007, la croissance était de 1564 % par an. Celle-ci ne cesse d'augmenter depuis. En 2009, on détectait près de 1 500 nouveaux malwares toutes les heures ! Les menaces sont souvent si complexes que La victime ne remarquera même pas que son ordinateur a été infecté ou que des données lui ont été dérobées.
Les principales menaces qui pèsent aujourd'hui sur les entreprises sont :
- Vol, détournement de données (fichiers clients, brevets, comptabilité, finance…)
- Corruption d'informations, suppression de fichiers.
- Paralysie du système d'information (et donc de son activité).

Suite à des actes de piratages ciblés, certaines entreprises ont même dû déposer le bilan, la perte ou la corruption de leurs données leur ayant été fatales.

Une sécurité souvent de niveau faible
Alors que la quantité d'informations stockées sous forme numérique atteint des records, il semble qu'il en soit de même en matière d'insécurité : près d'un informaticien sur deux (42%) considère que sa propre entreprise ne fait que peu de chose pour réduire les risques de vols ou de pertes de données confidentielles. Les résultats de l'enquête conduite auprès de 1000 spécialistes de la sécurité informatique en entreprise par le Ponemon Institute vont même encore plus loin : 45% d'entre eux reconnaissent qu'ils seraient dans l'impossibilité d'identifier, et donc d'avertir, les utilisateurs ou les clients dont les données personnelles auraient été volées.

Même si les directions de systèmes d'information ont fait quelques progrès ces dernières années, elles sont encore très loin d'avoir une culture sécurité suffisante pour protéger efficacement les données sensibles à caractère personnel ou confidentiel. Le choix jusqu'alors des entreprises a davantage été de protéger les équipements que les données elles-mêmes. Quant aux solutions installées, beaucoup se contentent d'un antivirus (pas toujours à jour), voire d'un pare-feu… et se croient protégées. Or, compte tenu de l'étendue des périphériques mobiles (clés USB, PDA, assistants personnels et téléphones mobiles) et de leur capacité de stockage (plusieurs dizaines de Go), la protection des données n'a pas suivi la mutation des technologies et des usages.

Les cybercriminels ont organisé un marché très juteux de revente sur Internet :
- Compte Paypal : 7$
- N° carte bleue (+code sécurité) : 7-25 $
- Carte de Sécurité Sociale : 100 $
- N° permis de conduire : 150 $
- N° carte crédit avec code PIN : 500 $

L'exploitation des failles de sécurité se monnaye aussi…
- Package malware : 1000 – 2000 $
- Exploit 1 heure : 1 $
- Exploit 5 heures : 4$
- Infection de 10 000 Pcs : 1000 $

Une sensibilisation aux risques « mitigée »
De l'avis des experts, la perception qu'ont les entreprises des risques auxquelles elles sont confrontées varie suivant la taille et les secteurs d'activité. Toutefois, comme le précise Olivier Pantaléo, Président de MAJJ, « *la plupart des entreprises n'arrivent pas à évaluer précisément l'ampleur des risques liés à la perte de données. Celle-ci peut engendrer des préjudices très importants pour l'entreprise.* » En effet, la perte ou le vol d'informations affectent aussi bien ses résultats, sa profitabilité que son image de marque. Et Michael Amselem, (Head of Europe Sales Division - End Point Solutions Check Point Software) d'ajouter : « *La perte de données représente également une perte de crédibilité pour une société qui n'aura pas pris les bonnes mesures pour éviter ce genre de fuite. L'exemple récent de Wikileak, par le biais de l'exposition de données sensibles, démontre une nouvelle fois l'ampleur des dégâts que ce genre de situations peut générer.* »

La protection des données n'est pas assurée comme elle devrait l'être et ce, malgré des législations parfois très sévères. « *Rares sont les entreprises qui ont réalisé la cartographie de leurs données sensibles* » poursuit Olivier Pantaléo. « *Seules celles qui ont des contraintes réglementaires fortes - comme le secteur banques, finances, assurances - ont classifié tout ou partie de leurs données et ont mis en place des mesures de sécurité au regard de leur classification.* » Ces entreprises font régulièrement des contrôles, se positionnant ainsi dans un 'cercle vertueux'. Elles sont donc plus matures que celles évoluant dans d'autres secteurs d'activité. Quand les entreprises n'ont pas de contraintes légales, pas d'amendes à la clé, elles font sans et continuent de faire sans. Ce que confirme Michael Amselem : « *Dans la plupart des cas, on a privilégié la répression et la crainte de celle-ci à l'encontre de l'éducation. Cela a induit une certaine passivité des entreprises du fait de leur incompréhension des solutions proposées et des impacts réels sur leur organisation en cas de perte de données. Trop souvent les entreprises s'équipent pour protéger leurs données après avoir subi un incident sévère.* »

La sensibilisation aux risques reste encore mitigée selon les entreprises. Selon une enquête menée par le CLUSIF en 2008, 20 % des interrogés pensent que les risques sont en forte baisse alors que 21 % pensent au contraire qu'ils sont en hausse, éventuellement très forte…

Données à caractère personnel, données d'entreprise
Comme nous le verrons dans le chapitre suivant, un environnement législatif, juridique existe bel et bien et ce, depuis 1978. Mais celui-ci encadre principalement les données à caractère personnel. A cet effet, qu'entend-on par « données personnelles » ? Maître Olivier Iteanu précise : « *Ce sont les toutes les données qui sont susceptibles d'identifier une personne physique. Nous avons deux types de données à caractère personnel : les données directes (nom, prénom…) et les données indirectes (plaque d'immatriculation de voiture, numéro de sécurité sociale…).* » On imagine aisément l'importance que représentent ces fichiers pour l'administration, les opérateurs télécoms, les hôpitaux et organismes de santé, les banques et assurances, la grande distribution, voire les services.

Certes, au regard de la Loi, les données à caractère personnel ont un statut particulier puisqu'elle concerne « la vie privée, l'intimité mais aussi la liberté » d'une personne. Pour autant, les données d'entreprise (comptes clients, comptabilité, paie, secrets de fabrication, brevets,…) sont des informations capitales pour son activité. Elles le sont aussi pour ses compétiteurs qui pourraient les exploiter à leur profit pour disposer, notamment, d'un avantage concurrentiel certain. Comment ? En mettant sur le marché un produit, un service ou une offre commerciale juste avant celle de son et ses concurrents. Cette avance sur le marché se mesure en millions d'euros mais aussi en notoriété.

Les exemples sont légion, dans l'industrie, la téléphonie mobile ou la grande distribution. Indéniablement, « l'espionnage industriel » s'est mis à l'heure du numérique.

Dans ce contexte, où les données à caractère personnel sont stockées et traitées aux côtés des données d'entreprise, la protection des données doit être d'autant plus renforcée qu'elle est, pour la première catégorie, entourée d'un cadre juridique complet et coercitif et, pour la seconde, vitale pour son fonctionnement et sa prospérité. L'ensemble de ces données doit être traité sur le même plan en matière de protection, avec la même vigilance et détermination face aux menaces ce que confirme Maître Isabelle Renard (Cabinet Racine) : « *Les données personnelles sont protégées comme le reste des données. Il y a dans la Loi Informatique et Liberté l'Article 34 qui est très important car il instaure « l'obligation de sécurité ». Les entreprises doivent veiller à ce que les données personnelles ne puissent pas être corrompues ou divulguées hors de l'entreprise. Dans les faits, cette obligation de sécurité n'est pas spécifiquement appliquée. L'entreprise protège ce type de fichiers comme elle protège le reste de ses documents. Si c'est bien fait, l'obligation de sécurité est remplie. Il est très rare qu'il y ait une spécificité technique autour de la protection des données personnelles.* »

Mais qu'en est-il sur le plan juridique de la protection des données autres que personnelles ? Maître Iteanu précise que « *c'est le code de la propriété intellectuelle qui s'applique ainsi qu'un certain nombre de textes un peu épars qui concernent les entreprises comme des dispositions générales du code pénal sur le secret des affaires, les secrets de fabrique. Mais il n'y a pas de régime général des données au sein de l'entreprise. On les traite en fonction de leur finalité. Si elles sont à caractère personnel, c'est la Loi de 1978 / 2004 qui s'applique. Si elles sont « originales » (littéraires, artistiques, musicales), on peut leur appliquer la Loi sur la propriété intellectuelle. Si elles touchent un investissement de l'entreprise (secret de fabrique), on parlera de savoir-faire.* »

II. Ce que dit la Loi…

La France dispose depuis 1978 d'un cadre juridique et législatif dédié à la protection des données à caractère personnel. Les Lois de 1978 et de 2004 ainsi que la Directive européenne de 1995 définissent un cadre législatif qui s'est enrichi avec l'évolution des technologies en matière de traitements et de diffusion des informations. Retour en arrière pour bien mesurer aujourd'hui l'importance pour les entreprises de connaître et respecter les textes en vigueur.

Le texte de référence en matière de protection des données est celui de la Loi n° 78-17 du 6 janvier 1978, « Loi relative à l'informatique, aux fichiers et aux libertés ».

➔ Cette Loi institue la Commission Nationale de l'Informatique et des Libertés (CNIL), autorité chargée de veiller à la protection des données personnelles et de la vie privée. Dans ce cadre, la CNIL vérifie que la Loi est respectée en contrôlant les applications informatiques, prononce des sanctions, établit des normes et propose au gouvernement des mesures législatives ou réglementaires de nature à adapter la protection des libertés et de la vie privée à l'évolution des techniques. A retenir l'article 34 : « Le responsable du traitement met en œuvre toutes mesures adéquates, au regard de la nature des données et des risques présentés par le traitement, pour assurer la sécurité des données et en particulier protéger les données à caractère personnel traitées contre toute violation entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation, la diffusion, le stockage, le traitement ou l'accès non autorisés ou illicites. »

Puis en 1981, le Conseil de l'Europe élabore la « Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » qui reste à ce jour, dans ce domaine, le seul instrument juridique contraignant sur le plan international, à vocation universelle, ouverte donc à l'adhésion de tout pays y compris non membre du Conseil de l'Europe.

➔ Cette Convention définit un certain nombre de principes pour que les données soient collectées et utilisées de façon loyale et licite. Ainsi, elles ne peuvent être collectées que dans un but précis et ne peuvent être utilisées de manière incompatible avec ce but ; elles doivent être exactes, proportionnées à cet objectif et conservées uniquement pendant le délai nécessaire à sa réalisation. Le texte établit, en outre, le droit d'accès et de rectification de la personne concernée et exige une protection spéciale pour les données sensibles (notamment celles concernant l'appartenance religieuse, les opinions politiques ainsi que les données génétiques ou médicales).

Dans le droit fil de cette Convention du Conseil de l'Europe, l'Union européenne a adopté en octobre 1995 la directive 95/46/CE qui constitue le texte de référence, au niveau européen, en matière de protection des données à caractère personnel.

➔ Cette directive met en place un cadre réglementaire visant à établir un équilibre entre un niveau élevé de protection de la vie privée des personnes et la libre circulation des données à caractère personnel au sein de l'Union européenne.

Pour ce faire, la directive fixe des limites strictes à la collecte et à l'utilisation des données à caractère personnel, et demande la création, dans chaque État membre, d'un organisme national indépendant chargé de la protection de ces données.

Tous les Etats membres ont maintenant transposé cette directive. Néanmoins, les actions entreprises au sein de l'UE restent encore insuffisantes pour faire face aux menaces que représentent le spam, les logiciels espions et les logiciels malveillants. Internet étant un réseau mondial, la Commission européenne souhaite développer le dialogue et la coopération avec les pays tiers concernant la lutte contre ces menaces et les activités criminelles qui y sont associées.

C'est sur la base de cette Directive que la Loi n°2004-801 du 6 août 2004 a été votée en deuxième lecture. Celle-ci modifie la Loi n° 78-17 du 6 janvier 1978 sur la protection des données au regard du traitement des données personnelles.

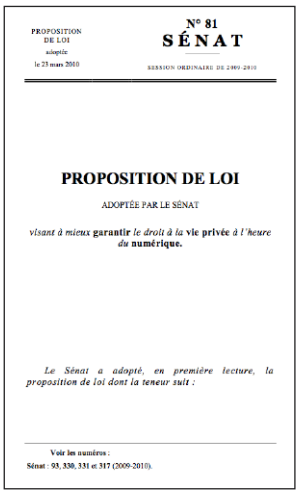
➔ Cette nouvelle Loi donne de nouveaux pouvoirs à la CNIL (sanctions) et de nouvelles opportunités pour les entreprises. Elle prend en compte les risques liés à l'utilisation des nouvelles technologies dans le cadre du traitement, de l'échange et de la circulation des données. Dans ces conditions, la Loi s'applique à l'ensemble des traitements de données à caractère personnel, c'est-à-dire à toute opération, quel que soit le procédé utilisé (la collecte, l'enregistrement, l'organisation, la conservation, l'utilisation, etc.) portant sur toute information relative à une personne physique identifiée ou pouvant être identifiée par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Cette Loi de 2004 limite le contrôle a priori des fichiers par la CNIL pour lui substituer le plus souvent un contrôle a posteriori. Les pouvoirs d'investigation ou d'accès aux données de la Commission ainsi que ses possibilités effectives d'intervention seront, en contrepartie, renforcées. La CNIL dispose de pouvoirs de sanction administrative graduée allant du simple avertissement jusqu'aux sanctions pécuniaires.

Plus récemment, le 23 mars 2010, le Sénat a adopté au Palais du Luxembourg, sans vote contraire, la proposition de Loi N° 93 (2009-2010) des Sénateurs Anne-Marie Escoffier et Yves Détraigne « visant à mieux garantir le droit à la vie privée à l'heure du numérique ».

➔ Cette proposition tend notamment, au travers de son article 7, à renforcer l'article 34 de la Loi informatique et libertés en rendant obligatoire la notification des failles de sécurité. En voici un extrait…

« En cas de violation du traitement de données à caractère personnel, le responsable de traitement avertit sans délai le correspondant informatique et libertés, ou, en l'absence de celui-ci, la Commission Nationale de l'Informatique et des Libertés (CNIL). Le responsable du traitement, avec le concours du correspondant informatique et libertés (CIL), prend immédiatement les mesures nécessaires pour permettre le rétablissement de la protection de l'intégrité et de la confidentialité des données. Le CIL en informe la CNIL. Si la violation a affecté les données à caractère personnel d'une ou de plusieurs personnes physiques, le responsable du traitement en informe également ces personnes,



PROPOSITION DE LOI
adoptée le 23 mars 2010

N° 81
SÉNAT
SESSION ORDINAIRE DE 2009-2010

PROPOSITION DE LOI

ADOPTÉE PAR LE SÉNAT

visant à mieux **garantir** *le droit à la* **vie privée** *à l'heure du* **numérique.**

Le Sénat a adopté, en première lecture, la proposition de loi dont la teneur suit :

Voir les numéros :
Sénat : 93, 330, 331 et 317 (2009-2010).

sauf si ce traitement a été autorisé en application de l'article 26. Le contenu, la forme et les modalités de cette information sont déterminés par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés. Un inventaire des atteintes aux traitements de données à caractère personnel est tenu à jour par le correspondant informatique et libertés. »

Maître Renard précise : « *Ce projet de Loi est actuellement en première lecture à l'Assemblée Nationale. Il n'a pas soulevé d'objections très importantes.* » On peut, dans ces conditions, imaginer que cette Loi sera adoptée courant 2011. Et Maître Itéanu d'ajouter : « *Internet c'est l'interopérabilité entre nous tous. La tendance de la jurisprudence est de nous rendre tous responsables les uns des autres. L'une des premières manifestations de cet esprit de responsabilité partagée est de rendre obligatoire - lorsque des données à caractère personnel sont conservées - la notification d'une faille de sécurité lorsque celle-ci est constatée. Si le système d'information d'une entreprise possède une faille qui lui est connue, et que celle-ci est susceptible de permettre l'évasion de données à caractère personnel, il y a obligation de la notifier à la CNIL pour que les personnes concernées soient informées.* »

Si cette Loi est adoptée, comme le sous-entendent les avocats interrogés, il restera à définir ses modalités d'application. Que devront précisément notifier ou omettre les entreprises face à une faille de sécurité ? Toujours est-il que les juristes s'accordent à reconnaître que cette directive a le mérite d'obliger les entreprises à mettre en place les moyens de protection réclamés. La réglementation américaine, pour sa part, indique que « si les données volées étaient chiffrées, il n'est pas nécessaire de faire de notification. » Nous verrons plus loin l'intérêt majeur pour les entreprises de chiffrer toutes leurs données, y compris pour les sociétés françaises.

La protection des données en Europe

Comme nous l'avons vu, En matière de protection des données personnelles, la France dispose d'un corpus de Lois important, en particulier la Loi de 2004 qui a rénové la Loi « Informatique et Liberté » de 1978. Mais qu'en est-il de la protection des données dans les autres pays européens ? Chaque pays a défini son autorité de supervision et un cadre législatif basé pour la plupart d'entre eux sur la Directive européenne de 1995. « *Le niveau de protection des données personnelles en Europe est maintenant uniforme au plan législatif, mais la protection effective dépend beaucoup des autorités administratives chargées du respect de la Loi. La CNIL, en France, est ainsi particulièrement active* » commente Maître Renard. « *La France est probablement l'un des pays du monde où la législation en la matière est la plus protectrice, et ce depuis le plus longtemps.* »

Il semble toutefois, au regard des nombreuses publications européenne en matière de protection des données, que les anglo-saxons avec leur autorité d'auto-régulation soient les plus actifs en matière de protection des données et de sanctions.

III. Les risques juridiques encourus

Comme nous l'avons vu dans le chapitre précédent, un cadre juridique existe pour les entreprises. Mais qu'en est-il lorsque l'une d'elle ne respecte pas les recommandations et réglementations en vigueur ? Qui est responsable ? Quelles pénalités ?

La responsabilité revient au chef d'entreprise

Au sein de l'entreprise, le responsable des données est son représentant légal. Généralement, c'est le dirigeant de l'entreprise, le mandataire social. « *Le non respect de la Loi Informatique et Libertés fait l'objet de sanctions financières et/ou pénales. Les sanctions pénales peuvent être appliquées à l'entreprise personne morale, et/ou à son dirigeant, et/ou un DSI ou un RSSI uniquement qui serait titulaire d'une délégation de pouvoir* » précise Maître Isabelle Renard, ce que confirme Maître Olivier Iteanu : « *Ce que nous constatons, c'est un système de délégation de pouvoir au sein de l'entreprise, le représentant légal cherchant à déléguer ses responsabilités pénales à des subalternes. Cela peut être le directeur général adjoint, le DSI, le RSSI.* » Mais cette délégation est encore timide.

Toujours est-il que le chef d'entreprise doit s'entourer de compétences dont la sécurité des informations et la protection des données est le métier. Le DSI et ou le RSSI peuvent le conseiller, l'avertir, l'alerter ou encore le sensibiliser, non pas par une approche technologique mais par une approche métier.

Des sanctions administratives, financières et pénales en cas de manquement

Lors de manquements sérieux au respect de la Loi Informatique et libertés, la CNIL a le pouvoir de prononcer des sanctions administratives ou financières (par Arrêt du Conseil d'Etat du 19 février 2008). Dans ce cas, la CNIL se réunit en formation contentieuse pour prononcer les sanctions prévues à l'article 45 de la Loi. Les sanctions pénales prévues aux articles 226-16 à 226-24 du Code pénal peuvent aussi s'appliquer, la CNIL ayant la possibilité de dénoncer au Procureur de la République les infractions à la Loi dont elle a connaissance.

Lorsque des manquements à la Loi sont portés à la connaissance de la formation contentieuse de la CNIL, celle-ci peut prononcer :

- Un avertissement à l'égard du responsable de traitement fautif, qui peut être rendu public.
- Une mise en demeure à l'organisme contrôlé de faire cesser les manquements constatés dans un délai allant de dix jours à trois mois. Si le responsable de traitement se conforme à la mise en demeure, la procédure s'arrête et le dossier est clôturé.

Si le responsable de traitement ne se conforme pas à la mise en demeure de la CNIL, la formation contentieuse peut prononcer, après une procédure contradictoire, durant laquelle le responsable de traitement incriminé peut présenter des observations orales :

- Une sanction pécuniaire (sauf pour les traitements de l'Etat), d'un montant maximal de 150 000€, et en cas de récidive, jusqu'à 300 000 € ; en cas de mauvaise foi, la CNIL peut ordonner l'insertion de la décision de sanction dans la presse.
- Une injonction de cesser le traitement.

- Un retrait de l'autorisation accordée en application de l'article 25 de la Loi.
- En cas d'urgence, l'interruption de la mise en œuvre du traitement, et le verrouillage des données pour trois mois.
- En cas d'atteinte grave et immédiate aux droits et libertés, le président de la CNIL peut demander, par référé, à la juridiction compétente, d'ordonner toute mesure de sécurité nécessaire.

La CNIL peut saisir le parquet qui est le seul à infliger une sanction pénale : jusqu'à 5 ans d'emprisonnement. « *La Loi prévoit des sanctions pénales dont je n'hésite pas à dire qu'elles sont ridiculement lourdes. C'est un des problèmes de cette Loi. Par exemple, un défaut de déclaration, c'est 2 ans de prison et 300 000 euros d'amende. Si l'on appliquait cette Loi, 80 % des patrons français seraient en prison. Il y a une disproportion importante entre la sanction et l'application de la Loi. Les sanctions sont rarement appliquées, ce qui ne les rend pas crédibles* » note Maître Renard… ce que confirme Maître Iteanu : « *L'activité pénale reste très faible : pas plus d'une vingtaine de jugements ont été rendus depuis 1978 par les Tribunaux et Cours d'Appels. Le volet pénal est là pour dissuader mais il est peu appliqué.* »

La principale sanction, c'est la publication et la publicité faite autour des décisions de la CNIL. Cela peut coûter très cher à l'entreprise (en particulier si celle-ci s'adresse au grand public) en termes d'image et de pourcentage de chiffre d'affaires perdu.

En juin 2010, la formation contentieuse de la CNIL a condamné la société JPSM pour l'envoi à des particuliers de fax publicitaires non-sollicités. Cette décision intervient après une sanction pour des faits identiques en 2007. C'est la première fois que la CNIL fait usage des pouvoirs dont elle dispose pour condamner la réitération de manquements à la loi Informatique et Libertés.

Un coût élevé pour l'entreprise
Quel est le coût de cette perte de données ? Qu'ont payé les entreprises face à leurs manquements au regard de leur législation respective ? Voici ce qu'ont du payer les entreprises à l'organisme de régulation pour non respect de la Loi :
- 6,75 Milliards d'euros Aux Etats-Unis (en hausse de 2% par rapport à 2008)
- 2,58 Milliards d'euros en Allemagne (en hausse de 7% par rapport à 2008)
- 1,68 Milliards de livres sterling au Royaume-Uni (en baisse de 3% par rapport à 2008).

On se souvient le cas de cette institution financière anglaise, la Nationwide Building Society, qui a été condamnée par la Financial Services Authority (FSA) à verser une amende de 980 000 £ à la suite du vol d'un de ses ordinateurs portables contenant des données de ses clients sans protection adéquate. On notera en particulier que la CNIL, le juge pénal ou la FSA, sanctionnent l'absence de mesures appropriées de sécurité en tant que telle, sans pour autant qu'un tiers, mal intentionné ou non, accède aux données.

FSA

Etre en conformité avec la Loi
Que faire pour respecter la Loi ? Les entreprises doivent procéder à un audit des traitements de données personnelles dont elles sont responsables, le cas échéant avec l'assistance de conseils spécialisés. Elles peuvent aussi nommer un « Correspondant aux Données Personnelles » (CDP).

« *Cet interlocuteur permet à l'entreprise d'être dispensée des déclarations simples. Mais personne dans l'entreprise n'est très chaud pour être CDP, notamment du fait d'un certain manque de clarté quant à son indépendance. De ce fait, il n'y en a pas beaucoup* » souligne Maître Renard.

Les entreprises peuvent également s'informer sur le site de la CNIL. « *Son site Web est l'outil d'information par excellence, bien fait, bien écrit, assez clair. Chaque année, la CNIL établit un rapport de très bonne tenue qui permet de se tenir informé de l'état des questions et de leur évolution* » ajoute Maître Iteanu qui constate que le respect de la Loi par les entreprises françaises est en progression, en particulier ces dernières années du fait du pouvoir de sanction accru de la CNIL.

IV. Bonnes pratiques

Pour être et rester en conformité avec le cadre juridique et les réglementations en vigueur, l'entreprise doit définir et appliquer des processus visant à renforcer la protection des données. « *Dans un premier temps, il est primordial pour l'entreprise d'avoir une vue claire des obligations qui s'appliquent à son environnement. Puis, en fonction de celles-ci, elle identifie les données à protéger. Il est ensuite plus aisé pour elle de mettre en œuvre des plans de protection adaptés sur le périmètre qui a été défini* » souligne Olivier Pantaléo (MAJJ). « *Il faut rappeler que le premier reproche fait à l'entreprise est le manquement à son obligation de moyens. C'est en somme une négligence qui est punie par la Loi.* »

Tous les experts, de la CNIL aux intégrateurs spécialisés en sécurité informatique, proposent aux entreprises de suivre les bonnes pratiques suivantes.

1. Réaliser une étude des risques
L'étude des risques permet de déterminer des mesures de sécurité à mettre en place. Elle doit être formalisée dans un document complet. Il convient donc de prévoir un budget pour leur mise en œuvre. Cette étude devra être mise à jour de manière régulière selon les évolutions du contexte et doit :

• Recenser les fichiers et données à caractère personnel (ex : fichiers client, contrats...) et les traitements associés, automatisés ou non, en identifiant les supports sur lesquels reposent ces traitements :
  - les matériels (ex : serveur de gestion des ressources humaines, CD-ROM...) ;
  - les logiciels (ex : système d'exploitation, logiciel métier...) ;
  - les canaux de communication (ex : fibre optique, Wifi, Internet...) ;
  - les supports papier (ex : document imprimé, photocopie...).

• Étudier les menaces qui pèsent sur chaque support et les hiérarchiser selon leur probabilité d'occurrence (vraisemblance). Exemples de menaces : vol d'un PC portable, contagion par un code malveillant, saturation des canaux de communication, photocopie de documents papier...).

• Étudier les risques :
  - Combiner chaque impact avec les menaces qui le concernent.
  - Hiérarchiser les risques ainsi obtenus selon leur gravité et leur vraisemblance.

• Mettre en œuvre des mesures de sécurité
Déterminer les mesures de sécurité pour réduire, transférer ou éviter les risques.

En fonction des moyens disponibles, il peut également être utile de prévoir la formation des personnes chargées de réaliser les études de risques et un audit sécurité du système d'information.

2. Protéger les postes de travail
La protection des postes de travail passe par la mise en œuvre de mesures pour prévenir les tentatives d'accès frauduleux, l'exécution de virus (ou autres malwares) ou encore la prise de contrôle à distance, notamment via Internet.

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Voici quelques précautions élémentaires :
- Installer un «pare-feu» (firewall) logiciel, et limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail.
- Utiliser des antivirus régulièrement mis à jour (souvent de façon automatique).
- Chiffrer les données (voir plus loin).
- Prévoir une procédure de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné.

3. Sécuriser l'informatique mobile

La multiplication des ordinateurs portables, des clés USB et des smartphones rend indispensable d'anticiper la possible perte d'informations consécutive au vol ou à la perte d'un tel équipement. La précaution élémentaire est de prévoir des moyens de chiffrement pour les espaces de stockage des matériels informatiques mobiles (ordinateur portable, périphérique de stockage amovible tels que clés USB, CD-ROM, DVD-RW, etc.).

Parmi ces moyens, on peut citer :
- le chiffrement du disque dur dans sa totalité au niveau matériel ;
- le chiffrement du disque dur dans sa totalité à un niveau logique via le système d'exploitation ;
- le chiffrement fichier par fichier ;
- la création de conteneurs (fichier pouvant contenir plusieurs documents) chiffrés.

Le chiffrement, parfois improprement appelé cryptage, est un procédé cryptographique permettant de garantir la confidentialité d'une information. Les mécanismes de cryptographie permettent également d'assurer l'intégrité d'une information, ainsi que l'authenticité d'un message en le signant.

En résumé

L'entreprise qui souhaite renforcer la protection de ses données et rester en conformité avec la réglementation en vigueur doit (sur les conseils de la CNIL) :
1. Analyser les risques
2. Authentifier les utilisateurs
3. Gérer les habilitations & sensibiliser les utilisateurs
4. Sécuriser les postes de travail
5. Sécuriser l'informatique mobile
6. Sauvegarder et prévoir la continuité d'activite
7. Encadrer la maintenance
8. Tracer les accès et gérer les incidents
9. Protéger les locaux
10. Protéger le réseau informatique interne
11. Sécuriser les serveurs et les applications
12. Gérer la sous-traitance
13. Archiver
14. Sécuriser les échanges avec d'autres organismes

V. Solutions

Plusieurs solutions permettent aux entreprises de protéger l'ensemble de leurs données, de contenir la perte de données et la fuite d'informations tout en restant en conformité avec les réglementations en cours. Leader mondial dans le domaine de la sécurité informatique, Check Point Software propose aux entreprises un vaste panel de logiciels pour protéger toutes les composantes du système d'information, de la passerelle Internet aux postes de travail. Parmi celles-ci, Endpoint Security, Full Disk Encryption / Media Encryption mais aussi Check Point Abra et ou encore la Software Blade DLP.

Protéger son poste de travail contre les menaces Internet
Les menaces Internet se multiplient en nombre et en complexité. Nombre d'entre elles ont été conçues par les cyber-criminels pour dérober les informations sensibles et confidentielles stockées sur le PC des collaborateurs. Check Point Endpoint Security protège les utilisateurs contre l'étendue des menaces Web, empêchant les logiciels malveillants d'accéder ou de contaminer leur poste de travail. Les utilisateurs sont entourés d'une « bulle de sécurité » quand ils surfent sur le Web, qui rend le système de protection transparent pour eux. Respectant une règle de sécurité très simple, similaire à celle d'un pare-feu, tous les téléchargements autorisés peuvent être réalisés, mais pas ceux qui ne sont pas sollicités. Ceci permet aux utilisateurs de naviguer sur n'importe quel site Web et de cliquer sur n'importe quel lien sans aucune crainte. Tous les comportements inconnus ou changements non sollicités (attaque du navigateur, logiciels espions et les virus) sont dirigés vers un système de fichiers virtualisé, et seuls les contenus désirés par l'utilisateur sont téléchargés et stockés sur son poste.

Par ailleurs, pour éviter que les utilisateurs se retrouvent piégés sur des sites frauduleux (versions falsifiées de « vrais » sites Web), la technologie WebCheck utilise un moteur anti-Phishing bimodal constitué à la fois d'une base de signatures de Phishing et d'une détection heuristique avancée.

Chiffrer ses données
Oublier son ordinateur portable dans un taxi ou un train, un aéroport ou un hôtel est très courant. Cette perte est un préjudice important pour l'entreprise qui voit dans cette disparition la mise à disponibilité d'autrui de données souvent sensibles : fichiers clients, brevets, renseignements personnels… Aussi, pour éviter toute utilisation frauduleuse des précieuses informations, une seule solution : chiffrer son PC.

Check Point Full Disk Encryption offre de nombreuses fonctionnalités pour chiffrer la totalité de son PC de bureau ou de son ordinateur portable :
- Chiffrement intégral du disque et authentification preboot
- Gestion de politique centrale, récupération de clé et assistance à distance
- Fonctionnement automatique et transparent pour l'utilisateur final
- Authentification performante et options de single sign-on
- Common Criteria EAL4, FIPS 140-2 et autres certifications clés
- Compatible avec les environnements Windows, Mac OS X et Linux

Grâce à Check Point Full Disk Encryption, l'ordinateur protégé devient inexploitable par toute personne non autorisée.

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Avec l'emploi généralisé des supports mobiles (comme les clés USB) qui contiennent désormais plusieurs giga-octets de données, il est aussi très important de chiffrer ce type de périphérique avec la solution Check Point Media Encryption. Celle-ci chiffre entièrement les données contenues de sorte qu'elles ne puissent être lues et exploitées que par son possesseur. En cas de perte, la clé ne peut délivrer ses secrets…

Protéger son environnement de travail

Accéder à son environnement de travail (applications et fichiers d'entreprises) en déplacement ou de chez soi est très pratique pour pouvoir continuer à travailler, notamment en cas de pandémie ou de conditions météos… Mais comment garantir la sécurité des données consultées ?

Check Point Abra est la solution adéquate pour les entreprises qui veulent doter leurs utilisateurs nomades d'un outil aussi pratique qu'efficace pour accéder et exploiter en toute sécurité les données du système d'information. Se présentant sous la forme d'une clé USB, elle fournit une connectivité sécurisée à partir d'un poste banalisé et contrôle toutes les opérations effectuées dans cet environnement ainsi que tous les accès au système d'information. Un identifiant et mot de passe sont nécessaires pour déverrouiller la clé et afficher le bureau virtuel ; celui-ci donne accès aux données chiffrées de l'utilisateur stockées sur la clé mais aussi au système d'information de l'entreprise pour lire ses emails, se connecter à l'intranet, accéder à ses fichiers, les traiter puis les stocker sur la clé USB ou encore lancer certaines tâches (impression, copier/coller...) tout en empêchant toute tentative d'intrusion ou de récupération de frappes clavier (keylogger) par des codes malveillants. Une fois la session terminée, aucune trace (fichiers, historique) ne subsiste sur le PC hôte.

Abra est la solution idéale pour les entreprises qui souhaitent mettre en place un plan de continuité d'activité (pour faire face, par exemple, à une épidémie) ou encore donner la possibilité à des partenaires de se connecter à son réseau (par exemple, pour de la tierce maintenance applicative).

Contenir les fuites d'informations

La fuite de données (DLP - Data Loss Prevention) est devenue pour les entreprises un enjeu tout aussi important que la protection de ses informations. Celle-ci se produit quasi-quotidiennement via la messagerie d'entreprise à la suite d'erreurs « banales » : envoi par email de données sensibles à un mauvais destinataire, ajout d'une pièce jointe différente de celle prévue... Les exemples sont hélas nombreux. Ces fuites d'informations, non intentionnelles dans 90 % des cas, peuvent toutefois causer des préjudices importants pour l'entreprise… Que faire alors pour endiguer ce phénomène courant ?

La Software Blade DLP de Check Point dote les entreprises d'un dispositif qui leur permet d'assurer une protection préemptive contre toute perte involontaire de données confidentielles. A cet effet, la lame logicielle DLP embarque un moteur de corrélation multi-données MultiSpect qui garantit une identification extrêmement précise des violations de données. Elle intègre également la technologie UserCheck™ qui avertit les collaborateurs en cas de danger, par e-mail ou à l'aide de fenêtres d'alerte. Ceux-ci sont alors invités à résoudre le problème rapidement avant la violation effective des données. Cette solution contribue grandement à la sensibilisation des utilisateurs et à la résolution de problèmes futurs.

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Pourquoi choisir les solutions Check Point ?

Réponse en trois points…

- Check Point leader dans la protection des données mobiles
  Depuis sa création en 1993, Check Point Software consacre la totalité de son activité à la protection du système d'information et des données. Leader dans le domaine de la sécurité informatique, Check Point Software ne cesse d'innover – dans le respect des standards – pour garder en permanence un temps d'avance sur ses compétiteurs.

- Un savoir-faire reconnu mondialement
  Dans sa toute récente étude dédiée à la protection des données mobiles, le Gartner a positionné Check Point Software comme l'un des leaders de son Magic Quadrant. Selon l'Institut de recherche, Check Point est hautement reconnue par les clients et les analystes pour l'étendue de sa gamme dédiée à la protection des données. La nouvelle solution Check Point Abra a également montré la capacité de Check Point à innover dans le domaine de la protection des données mobiles.

- Des solutions de sécurité éprouvées, pensées pour les utilisateurs
  La plupart des solutions du marché nécessite une connaissance informatique importante et sollicite l'utilisateur à de nombreuses reprises, au détriment de sa productivité. Plusieurs technologies mises en œuvre par Check Point contribuent à un usage transparent de la protection en place. Tel le mécanisme de Single-Sign-On (SSO) qui permet de s'identifier une seule fois, au démarrage du PC. Cette même authentification sert à la fois à déchiffrer le disque, démarrer la session Windows, établir la connexion VPN, chiffrer les données sur les médias amovibles, etc. Au final, l'utilisateur ne s'aperçoit pas de ce besoin d'identification. La fonctionnalité de SSO est intégrée dans la solution Check Point Endpoint Security sur tous les composants d'authentification. Check Point Abra joue également la carte de la performance et de la transparence via une authentification unique (pour déchiffrer le media et afficher le bureau virtuel) et un certificat digital qui rend transparente la connexion VPN sans nécessiter une nouvelle authentification. L'utilisateur gagne ainsi en rapidité et en confort.

« *Pour Check Point, la sécurité doit avant tout passer par l'éducation et la compréhension de nos clients des enjeux et des risques potentiels encourus en cas de non respect des règles de sécurité. Nous observons que certaines entreprises sont encore réticentes à implémenter certaines technologies de peur d'impacter directement le poste de travail. La compréhension de ces besoins nous a amené à développer des solutions simples à utiliser avec un agent unique End Point couvrant tous les aspects de protection. Ces solutions sont faciles à implémenter et préservent l'environnement de l'utilisateur sans altérer ses performances. Elles sont également administrables à distance depuis une console de management unique ; celle-ci gère l'ensemble des composants, en assure le déploiement et applique les règles de sécurité en parfaite cohérence pour l'ensemble de l'entreprise* » conclut souligne Michael Amselem.

VI. Références

La CNIL
La Commission Nationale de l'Informatique et des Libertés (CNIL) a été instituée par la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en 2004, qui la qualifie d'autorité administrative indépendante.

La CNIL a pour mission essentielle de protéger la vie privée et les libertés dans un monde numérique. Ses missions peuvent se résumer en quatre mots : informer, conseiller, réguler et recenser.

La commission se compose d'un collège pluraliste de 17 personnalités : 4 parlementaires (2 députés, 2 sénateurs), 2 membres du Conseil économique et social, 6 représentants des hautes juridictions (2 conseillers d'Etat, 2 conseillers à la Cour de cassation, 2 conseillers à la Cour des comptes), 5 personnalités qualifiées désignées par le Conseil des ministres (3), le Président de l'Assemblée nationale (1) et le Président du Sénat (1).

La CNIL en chiffres
Chaque année :
• 72 000 traitements déclarés
• 120 000 appels téléphoniques
• 25 000 courriers reçus
• 5 000 plaintes ou demandes de conseil
• 200 contrôles
• 13 millions d'€ de budget

La CNIL a édité le guide « La sécurité des données personnelles » à l'attention de tous les responsables de traitement ainsi qu'à toute personne disposant d'un minimum de connaissances informatiques (administrateur système, développeur, responsable de la sécurité des systèmes d'information, utilisateur...) et souhaitant évaluer le niveau de sécurité dont doit bénéficier tout traitement de données à caractère personnel.

Vous pouvez vous le procurer sur le site de la CNIL :
www.cnil.fr

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Maître Isabelle Renard

Isabelle Renard a rejoint le Cabinet Racine en qualité d'associé en 2010. Avocat et Docteur Ingénieur, elle a développé au cours de sa carrière une forte expertise des aspects juridiques et stratégiques des technologies de l'information, qui s'appuie sur son expérience professionnelle dans l'industrie de l'électronique et des services. Elle anime une équipe dédiée à la protection et à la défense des actifs incorporels des entreprises, qui couvrent tant au conseil qu'au contentieux les domaines de compétence suivants :

- Les contrats industriels, commerciaux et informatiques
- Le droit de la propriété intellectuelle (logiciels et actifs immatériels de l'entreprise).
- Les contentieux de brevets
- La sécurité Informatique, la dématérialisation des échanges et l'archivage numérique.
- La protection des données personnelles
- Le droit de l'Internet
- L'intéressement des salariés à leurs créations et inventions.

Expert IFEJI (Institut Français d'experts juridiques internationaux) et membre de la FEDISA (Fédération ILM, stockage, Archivage), Isabelle Renard exerce en outre une importante activité d'enseignement et est l'auteur d'ouvrages et de nombreux articles dans la presse spécialisée et générale. Elle est membre du conseil d'administration de l'AFAI (Association Française des auditeurs informatiques) et de FEDISA. www.racine.eu

Maître Olivier Iteanu

Maître Olivier ITEANU est Avocat à la Cour d'Appel de Paris depuis Décembre 1988. Il est également chargé d'enseignement à l'Université de Paris XI (Faculté Jean Monet), dans les Master 2 (DESS) du droit du numérique, du droit des activités spatiales et des télécommunications, de la gestion de l'information ainsi qu'à l'Université de Paris I Sorbonne dans le Master droit de l'administration électronique. Il est le fondateur et dirigeant de la société d'Avocats, la Selarl ITEANU.

Olivier Iteanu est l'auteur de nombreux ouvrages dont « Internet et le droit - aspects juridiques du commerce électronique » (premier ouvrage de droit français traitant de l'Internet » paru aux Editions Eyrolles en Avril 1996) ainsi que « Tous cybercriminels » paru aux éditions Jacques-Marie LAFFONT EDITION en Avril 2004 et de « L'identité numérique en question » (Editions Eyrolles - Mars 2008).

Il est responsable du module de formation droit de l'informatique de l'École Française des Barreaux à Paris pour la formation des Avocats stagiaires et réalise des interventions dans le cadre du module « Nouvelles Technologies et Droit » devant les auditeurs de Justice de l'École Nationale de la Magistrature à Bordeaux ainsi que devant les magistrats en formation permanente à Paris. Olivier Iteanu dispense des formations sur les contrats informatiques pour le Groupe LAMY, sur les aspects juridiques d'Internet pour EFE et sur la sécurité informatique auprès des professionnels pour le Groupe RISC TECHNOLOGY.
www.iteanu.com

MAJJ
Expert en sécurité de l'information, MAJJ accompagne les entreprises dans l'intégration et le déploiement de solutions à valeur ajoutée afin de répondre aux exigences des normes telles que PCI DSS ou encore ISO2700X.

Présent sur tous les secteurs d'activités, MAJJ apporte à ses clients son expertise ainsi que des solutions clés en main pour répondre aux contraintes normatives et réglementaires, et ce, à travers deux offres :

Déploiement et Intégration
- Etude, Ingénierie et expertise
- Mise en œuvre de solutions
- Transfert de compétences

Services Managés
- Support aux utilisateurs
- Exploitation & Administration
- Hotline et traitement des incidents

Les principaux atouts de MAJJ sont son expertise en matière de sécurité et de conformité, sa souplesse et sa réactivité (service sur mesure dans des délais très brefs) ainsi qu'une grande connaissance des environnements informatiques complexes. www.majj.fr

Ressources / Livres Blancs
- Livre Blanc sur le DLP :
http://france.checkpoint.com/uploads/white-papers/dlp-whitepaper-fr.pdf

- Livre Blanc sur Check Point Abra :
http://france.checkpoint.com/index.php?page=abra_form

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints, unified under a single management framework. Check Point provides customers uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented Stateful Inspection technology. Today, Check Point continues to innovate with the development of the software blade architecture. The dynamic software blade architecture delivers secure, flexible and simple solutions that can be fully customized to meet the exact security needs of any organization or environment. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

CHECK POINT OFFICES

Worldwide Headquarters
5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-624-1100
email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: http://www.checkpoint.com

Janvier 2010