



Un livre blanc Websense®

La sécurité informatique et la conformité réglementaire

Le mot d'accueil de Websense

L'ouverture du système d'information vers l'extérieur, voilà le défi majeur de l'entreprise d'aujourd'hui.

En effet, cette évolution s'accompagne de nouveaux risques juridiques pour les dirigeants, responsables et cadres de l'organisation.

Contrôler les nouveaux usages pour sanctionner les abus sans porter atteinte aux droits les plus élémentaires de la personne, c'est le défi qui doit être relevé par l'entreprise.

La Société WEBSense accompagne les entreprises européennes dans leur démarche. Elle le fait, tout d'abord, en leur permettant d'apprécier la nouvelle situation juridique créée pour faire, ensuite, le choix d'une organisation adaptée à l'enjeu, au moyen, notamment, des outils techniques du marché.

Aussi, notre Société s'est adressée à l'un des Cabinets d'Avocats les plus en pointe en France et en Europe sur ces questions pour réaliser ce livre blanc.

Elle lui a demandé de restituer une information honnête, fidèle et surtout accessible aux non juristes.

Elle lui a donné accès aux meilleurs experts pour compléter sa propre information, tant les nouvelles questions posées exigent une collaboration étroite entre l'organisation, la technique et le juridique.

Ce premier pari nous semble avoir été réussi et nous vous proposons d'en prendre connaissance sans modération.

Bonne lecture !

Websense France

Introduction	1
Les origines de la Conformité réglementaire « Compliance »	1
La « Compliance » impose d'identifier tout d'abord les règles auxquelles l'entreprise doit se plier	1
La multiplication des chartes d'usage de l'internet au sein des entreprises	2
Les impacts de la Loi Sarbanes-Oxley et de l'Accord Bâle II en France	4
Chapitre 1 : Les menaces développées au sein de l'entreprise	6
Section 1 - La détention de fichiers pédophiles téléchargés sur le serveur de l'entreprise (proxy de navigation sur le web)	6
Section 2 - Un salarié télécharge sur le lieu de travail des fichiers musicaux pirates en P2P	7
Section 3 - Un employé exporte sans autorisation des informations couvertes par le secret de fabrique	9
Section 4 - un salarié consulte des sites pornographiques de son domicile au moyen de l'ordinateur portable de l'entreprise	10
Section 5 - Copies illicites de logiciels sur les postes de travail	10
Chapitre 2 : Les menaces venant de l'extérieur	12
Section 1 - La base de données client pillée par des tiers étrangers à l'entreprise : Président, Rssi et Cadres face à leurs juges	12
Section 2 - l'entreprise impliquée par des propos diffamatoires sur Internet	13
Section 3 - Un virus déposé sur le site Web de l'entreprise qui devient une passerelle de propagation	14
Section 4 - L'identité de l'entreprise usurpée	15
Section 5 - l'attaque rebond et poste zombie	17
Conclusion	19

Introduction

Les origines de la Conformité réglementaire « Compliance »

Issue de la pratique anglo-saxonne et de la déontologie, la « Compliance » correspond à la mise en place de stratégies propres destinées à assurer un comportement conforme « aux règles du jeu ».

Cette notion de « Compliance » était à l'origine surtout liée à l'activité bancaire et au respect des règles concernant le délit d'initié. Pour éviter un éventuel engagement de la responsabilité des banques pour des actes commis par leurs employés, ces dernières se dotèrent de règles de comportements internes ou « Compliance Codes » visant à prévenir un tel risque. Ainsi, les premières références à ce concept se trouvent dans les « guidelines » des grandes banques d'investissement aux États-Unis, au début des années quatre-vingt.

Aujourd'hui, le concept de « Compliance » ne se limite plus seulement au respect par les banques de la législation pénale relative aux délits d'initiés mais fait référence au respect de toutes les lois et les règles applicables, ainsi qu'aux codes de conduite et standards de bonnes pratiques, qu'ils soient internes ou externes et quelque soit le type d'entreprise.

En outre, cette notion de « Compliance » recouvre une dimension éthique, composée de valeurs sociales et morales allant au-delà des normes strictement légales.

La « Compliance » impose d'identifier tout d'abord les règles auxquelles l'entreprise doit se plier

La « Compliance » se définit comme un concept d'organisation au sein d'une entreprise qui garantit que celle-ci respecte les lois, les règlements, les codes de conduite, ainsi que les standards de bonne pratique.

En tant que fonction d'organisation dans une entreprise, la « Compliance » est un instrument de surveillance de la gestion interne de l'entreprise afin de s'assurer de la mise en conformité de l'entreprise avec la réglementation, les normes et l'éthique de l'entreprise.

Ce système de contrôles internes recouvre également la gestion des risques auxquels l'entreprise doit faire face dans ses activités de tous les jours. En effet, la non-conformité aux règles, qu'il s'agisse de lois, de règlements internes ou de règles déontologiques, expose une entreprise à l'engagement de sa responsabilité ainsi qu'à un éventuel risque pesant sur sa réputation.

Pour s'assurer de la conformité aux lois et autres règles normatives, une entreprise doit tout d'abord déterminer précisément quels sont les risques potentiels auxquels elle doit faire face et par conséquent identifier le corps de réglementation à laquelle cette dernière est soumise.

En d'autres termes, appliqués à la sécurité informatique, la « Compliance » correspond à l'identification d'un ensemble de règles que l'entreprise doit respecter.

C'est seulement après cette analyse qu'il convient de rédiger des règles normatives internes, sous forme de politiques, de directives, ou encore de codes de conduite contenant des règles claires, facilement compréhensibles, ainsi que les droits et obligations clairement définies à l'intention des salariés.

C'est dans ce contexte qu'il est apparu progressivement des chartes d'usage d'Internet visant à informer les salariés de leurs droits et obligations quant aux modalités d'utilisation de l'internet afin de les responsabiliser.

La multiplication des chartes d'usage de l'internet au sein des entreprises

A l'origine, outil exclusivement à destinée pédagogique, certains employeurs tentent désormais d'élever les chartes au niveau d'une norme juridique, c'est-à-dire une norme contraignante et susceptible de sanction en cas de violation.

Pour ce faire, la charte doit être intégrée dans une des normes juridiques contraignante déjà existante dans le monde du travail, c'est-à-dire, soit le règlement intérieur de l'entreprise, unilatéralement écrite par l'employeur soit le contrat de travail de l'employé, norme juridique individuelle.

Dans ce cas, effectivement, l'employeur devra démontrer que son salarié a accepté la charte, d'où l'usage consistant à la faire signer.

Pour élaborer une telle charte, s'impose une conciliation nécessaire de deux principes : le droit reconnu à tout employeur de contrôler de la bonne exécution de leur travail par ses salariés et celui du salarié d'exiger le respect de sa vie privée même dans le cadre de son contrat de travail.

Le contrôle de l'employeur doit donc s'opérer sans porter atteinte à la vie privée de ses salariés.

Trois conditions sont donc nécessaires :

L'information préalable des salariés

S'abstenir de prévenir les salariés de la mise en place d'un système visant à contrôler l'usage qu'ils font d'internet (surf, envoi et réception d'e-mails...), entraînera l'irrecevabilité de toute preuve issue de ce système aux yeux de la loi.

En effet, l'article L. 121-7 du Code du travail stipule que :

« [...] le salarié est informé [...] des méthodes et techniques d'évaluation professionnelle mises en œuvre à son égard. Les résultats obtenus doivent rester confidentiels ».

La jurisprudence a consacré un principe posé par l'article L 121-8 du Code du travail qui précise qu' :

« Aucune information concernant personnellement un salarié ou un candidat à l'emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi. »

L'avis des organes représentatifs du personnel

L'article L. 432-2 du Code du travail stipule que « le comité d'entreprise est informé et consulté préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur [...] les conditions de travail du personnel ».

Par ailleurs, l'article 432-2-1 du Code du travail indique que « Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. »

Pour les entreprises de moins de 50 salariés, la discussion collective ne s'impose pas... mais la nécessité d'une information individuelle demeure.

La justification du contrôle : le respect du principe de proportionnalité

Prohiber purement et simplement toute utilisation individuelle d'Internet et instaurer de lourdes sanctions aux salariés contrevenants est une situation en pratique impossible à faire observer.

Selon le principe de proportionnalité, le dispositif de contrôle mis en place par l'employeur doit être justifié par un intérêt légitime.

Aux termes de l'article L.120-2 du Code de travail, « *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.* »

La Commission Nationale de l'Informatique et des Libertés (CNIL), de façon pragmatique a d'ailleurs reconnu qu' « *une interdiction générale et absolue de toute utilisation d'Internet à des fins autres que professionnelles ne paraît pas réaliste dans une société de l'information et de la communication* ». Ainsi, a-t-elle recommandé un « *usage raisonnable* », afin de garantir un accès normal au réseau Internet sans entraver la liberté d'action du salarié.

Pour confondre un employé, il faut donc prouver un usage personnel « excessif », « inadmissible » des moyens mis à sa disposition.

La preuve de l'utilisation abusive doit être clairement attribuée à une personne et non, exclusivement à un poste informatique, la présence d'un identifiant et d'un mot de passe personnel sur chaque machine facilite à ce niveau le recueil de la preuve.

C'est ainsi que le 14 décembre 2004, la Cour d'Appel de Metz a débouté un employeur qui n'avait pas réussi à identifier clairement le fautif, le poste étant partagé par plusieurs personnes.

Le monde du travail s'est laissé séduire et apprivoisé par les avantages sans précédent qu'offrent les technologies de l'information et de la communication.

Ainsi, l'entreprise est-elle devenue aujourd'hui un lieu privilégié de l'usage du réseau Internet.

La plupart des salariés disposent aujourd'hui d'un accès direct à l'internet ainsi que d'une messagerie électronique pour les besoins de leur travail. L'internet facilite les échanges, le transfert des informations et augmente de façon exponentielle la rapidité des communications.

Si cette ouverture du système de l'entreprise au réseau mondial se révèle un atout majeur en termes de rapidité et de coûts des transactions et diverses opérations commerciales, c'est malheureusement au prix d'une exposition encore plus directe et permanente aux nouvelles menaces qui se sont intensifiées et diversifiées.

Tout d'abord, au sein même de l'entreprise, l'usage à titre personnel par les salariés de l'internet peut se révéler lourde de conséquence : saturation des capacités de stockage des ordinateurs et des bandes passantes entraînant une perte de productivité, multiplications des risques de virus, atteinte à l'image de l'entreprise... et n'illustrent que quelques exemples des atteintes dont une entreprise peut être victime sans même dépasser son enceinte.

Le risque que courent les entreprises est d'autant plus grand que ces dernières peuvent être poursuivies sur le fondement de l'article 1384, alinéa 5 du Code civil si le préposé agit à l'occasion de ses fonctions et n'a pas excédé les limites de sa mission¹.

Ces hypothèses incitent les employeurs à contrôler de plus en plus scrupuleusement les flux d'informations entrants et sortants et circulant sur le réseau : contrôle des sites visités par les salariés, envois et réceptions d'e-mails, téléchargements...

A ces menaces de type « interne » s'ajoutent celles venant de l'extérieur, qui représente autant de nouveaux risques pour la sécurité de l'entreprise et son bon fonctionnement voire aussi son image dans les réseaux commerciaux.

Face à ce contexte de menaces multiples, quels contrôles de l'usage de l'internet, notamment sur la messagerie électronique ou sur l'accès à des sites, peuvent-ils instaurer pour concilier la protection de leur système informatique et de l'entreprise et les droits des salariés ?

Les impacts de la Loi Sarbanes-Oxley et de l'Accord Bâle II en France

La Loi Sarbanes-Oxley

Entrée en vigueur aux Etats-Unis en 2002, les dispositions de la Loi Sarbanes-Oxley (Loi SOX) visent à améliorer la transparence des comptes publiés par les entreprises et à renforcer la confiance dans la qualité de leur gestion.

Applicabilité

La Loi SOX s'applique aux sociétés, banques, organismes d'épargne et les sociétés anonymes non anonymes et cotées en bourses non américaines qui déposent des dossiers auprès de la SEC sous la section 13(a) ou 15(d) de la loi SEA (Securities Exchange Act) de 1934 et à toutes les filiales européennes d'entreprises américaines.

Toutes les sociétés cotées, dont la capitalisation boursière est supérieure à 75 millions de dollars et dont l'exercice se termine le ou après le 15 juin 2004 seront contraintes de déposer auprès de la SEC un rapport rédigé par la Direction portant sur le contrôle interne exercé sur le reporting financier en même temps que leur rapport financier annuel.

Pour les autres entreprises cotées et dont la capitalisation boursière est inférieure à 75 millions de dollars, la date est fixée au 15 avril 2005.

En Europe, au 1^{er} avril 2007, 306 sociétés sont directement concernées par la Loi SOX, dont 32 en France.

Les obligations légales fixées par la Loi SOX

La Loi SOX impose à toutes les entreprises cotées aux Etats-Unis, de présenter à la Commission américaine des opérations de bourse (SEC) des comptes certifiés personnellement par leur dirigeant.

Elle rend donc les dirigeants pénalement responsables des comptes publiés. Elle assure aussi et surtout l'indépendance des auditeurs face aux pressions dont ils peuvent être (et sont) l'objet de la part des dirigeants d'entreprise.

Il est important de noter que les systèmes d'information sont impliqués à double titre par la Loi SOX :

- d'une part, dans l'utilisation de l'informatique comme outil de gestion et de contrôle financier,
- d'autre part, dans l'obligation qui instituée (et c'est plus nouveau) d'assurer la sécurité de ce même système informatique.

Même si cette Loi ne s'applique pas directement en France, elle a fortement influencé les rédacteurs de la Loi sur la Sécurité Financière, dite Loi Mer, adoptée en juillet 2003.

En effet, à l'image de la Loi SOX, la Loi française vise à limiter les catastrophes financières résultant d'incuries ou d'actions de camouflages délictueux.

Elle emploie 3 moyens :

- accroître la responsabilité des dirigeants,
- renforcer le contrôle interne des systèmes informatiques,
- réduire les conflits d'intérêt.

L'Accord Bâle II

L'Accord Bâle II a pour objet de garantir que les établissements financiers gèrent le risque de manière à disposer des capitaux pour couvrir leur endettement.

Les objectifs de cet accord visent à améliorer la transparence, à réduire les risques de fraude et à empêcher la perte de clients ou les perturbations sur le marché en raison d'une gestion imprudente des risques.

Fondamentalement, la seule connaissance par l'entreprise des risques potentiels au sein de chaque entité opérationnelle ne suffit pas. Il faut également être en mesure d'évaluer, de gérer, de contrôler et de quantifier le risque opérationnel pour l'ensemble de la société.

L'Accord de Bâle sera mis en œuvre au sein de l'UE par le biais de la Directive sur l'adéquation des fonds propres.

A cet égard, Bâle II impose aux entreprises de publier cinq ans de données historiques, ce qui signifie que les prestataires de services financiers doivent avoir déjà collecté les données ou être en mesure de renseigner leurs bases de données de manière rétroactive.

En outre, depuis le 1er janvier 2004, les établissements financiers doivent prouver qu'ils utilisent un système de notation du risque conforme aux dispositions de Bâle II.

La conformité à Bâle II impose aux prestataires de services financiers de réaliser une étude fondamentale de leurs processus métier et de leurs systèmes informatiques afin de s'assurer qu'ils sont en mesure de contrôler et de surveiller leur exposition au risque de crédit.

Chapitre 1 : Les menaces développées au sein de l'entreprise

Section 1 - La détention de fichiers pédophiles téléchargés sur le serveur de l'entreprise (proxy de navigation sur le web)

Si les techniques de l'information et de la communication ont permis un échange de flux d'informations dont l'intensité et la diversité sont sans précédent, les contenus échangés sont malheureusement d'une qualité inégale.

En effet, avec l'internet, le réseau des entreprises s'est ouvert sur l'extérieur, notamment grâce aux emails et au Web. Cette ouverture s'est accompagnée d'une intensification des flux entrants et sortants qui s'échangent à partir ou à destination du système d'information de l'entreprise et est devenue progressivement un terrain propice au développement d'échanges porteurs de contenus illégaux, tels que ceux à caractère pédophile.

Dans l'ensemble de l'Europe, la détention d'images pédophiles voire la simple visite d'un site pédophile est sanctionnée pénalement.

En France, l'article 227-23 du Code Pénal punit et réprime :

« Le fait de (...) fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique ».

Ces infractions sont lourdement sanctionnées par des peines maximales de trois ans d'emprisonnement et de 75.000 euros d'amende.

Le même texte réprime « Le fait de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter (...) est puni des mêmes peines. »

Enfin, l'utilisation des moyens de télécommunications [communications électroniques] est même une circonstance aggravante prévue par la Loi :

« Les peines sont portées à cinq ans d'emprisonnement et à 75.000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de télécommunications. »

Enfin, lorsque ce délit est commis en bande organisée, les peines maximales sont portées à dix ans de prison et 500.000 euros d'amende.

Les gestes pour dénoncer et dégager sa responsabilité

Des fichiers pédophiles sur le serveur de l'entreprise posent la question de sa responsabilité, de celle de ses dirigeants sociaux (Président, Directeur Général, Gérant).

Sur le plan pénal, l'employeur n'engage sa responsabilité que s'il a intentionnellement participé à la commission de l'infraction.

En l'occurrence, l'hypothèse la plus courante serait que le salarié agit à l'insu de son employeur.

Néanmoins, un employeur dont on peut démontrer qu'il savait ou aurait du savoir que de telles pratiques s'étaient développées au sein de l'entreprise pourrait se voir reprocher des actes de complicité par fourniture de moyens. En outre, l'employeur subira en premier lieu les désagréments qu'implique une enquête de police ou une enquête judiciaire, tels que les perquisitions et saisies sur les lieux des machines utilisées. Aussi, mieux vaut donc pour l'employeur, ne pas courir ce risque et prendre le problème à bras le corps, c'est-à-dire s'en soucier, éduquer et contrôler que de telles pratiques n'ont pas cours.

Sur le plan civil, c'est-à-dire sur le plan d'un éventuel dédommagement des victimes, l'article 1384 alinéa 5 du Code civil dispose que « *les maîtres et les commettants² [sont responsables] du dommage causé par leurs domestiques et préposés³ dans les fonctions auxquelles ils les ont employés* ».

Selon la jurisprudence, l'employeur « *ne s'exonère de sa responsabilité que si son préposé a agi **hors des fonctions** auxquelles il était employé, **sans autorisation, et à des fins étrangères** à ses attributions* ».

Cependant, une jurisprudence française élaborée par la Cour de Cassation depuis 1998⁴, tend à considérer que l'employé a agi dans ses fonctions dès l'instant où le délit a pris place durant son temps de présence en entreprise et avec les moyens mis à sa disposition par son employeur.

Aussi critiquable que soit cette jurisprudence sur le plan de l'équité, car elle aboutit à obliger l'entreprise à dédommager, c'est-à-dire payer, des victimes pour des actes qu'elle n'a pas commis et auxquels elle n'a pas participé, il n'en reste pas moins que l'employeur risque d'être tenu pour responsable dans la mesure où il a donné au délinquant l'accès matériel et logiciel aux contenus pédophiles.

Face à tel danger, il est donc nécessaire d'organiser la traçabilité de l'ensemble des flux entrants et sortants qui circulent et s'échangent via les systèmes informatiques de l'entreprise.

Mais cette traçabilité connaît des limites que tout employeur doit respecter. Tout employeur doit respecter la boîte électronique de son salarié.

Le célèbre « arrêt Nikon » rendu par la Cour de cassation le 2 octobre 2001 a encadré très strictement le droit d'accès au contenu d'un mail :

« [...] *Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de la liberté fondamentale, prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition [...] et cela même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur.* »

La Chambre Commerciale de la Cour de Cassation a réaffirmé de façon claire sa position dans un arrêt du 17 mai 2005:

« *l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de celui-ci ou celui-ci dûment appelé* ».

Section 2 - Un salarié télécharge sur le lieu de travail des fichiers musicaux pirates en P2P

Contrairement à une idée répandue, le Peer To Peer ou P2P n'est pas illégal en soi. C'est même probablement une technique d'échange, qui correspond à l'esprit d'universalité et de partage prôné par les pionniers de l'Internet et qui est promis à un grand avenir car elle va permettre au niveau professionnel des échanges entre membres d'une même entreprise ou entre entreprises.

Le P2P ne devient illégal qu'à partir du moment où les fichiers qui s'échangent sont eux-mêmes illégaux.

C'est tout le problème de cette technique d'échange.

Car interdire le P2P a priori serait absurde voire contre productif.

¹ Entendez, les « employeurs »

² Entendez les « employés »

³ Tribunal correctionnel du Mans du 16 février 1998

En revanche, on ne peut nier qu'il est un usage établi bien qu'illégal consistant à échanger des fichiers le plus souvent musicaux et vidéos au moyen de cette technique, qui sont des copies pirates.

Est une copie dite pirate, une musique téléchargée sans que le titulaire des droits (compositeur, éditeur, artiste interprète notamment ci-après les auteurs) sur cette musique ait donné son accord préalable au téléchargement.

En effet, il ne faut pas oublier que certains auteurs consentent de diffuser leurs œuvres au moyen de cette technique. Il en résulte que les internautes sont en droit de les télécharger par le P2P.

En revanche, dès lors qu'un internaute télécharge des fichiers musicaux sans l'autorisation de leurs auteurs, celui-ci se rend coupable du délit de contrefaçon.

Selon l'article L. 122-4 du Code de la propriété intellectuelle (CPI) « *toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite* ».

L'article L 335-3 du CPI sanctionne « *toute reproduction ou représentation par diffusion, par quelque moyen que ce soit* » tandis que l'article L 335-4 du même Code sanctionne toute « *fixation, reproduction, communication ou mise à disposition du public, à titre onéreux ou gratuit (...) d'un phonogramme, réalisée sans l'autorisation, lorsqu'elle est exigée de l'artiste interprète.* »

Ce téléchargement « *illicite* » est condamné par l'article L 335-2 du Code de la Propriété Intellectuelle des peines maximales de trois ans d'emprisonnement et 300.000 euros d'amende (peines aggravées par la Loi Perben II).

Le délit et les peines associées s'appliquent également à celui ou celle qui a mis le fichier en partage, c'est à dire qui a offert un fichier piraté au téléchargement des internautes, et cela vaut pour tous les types d'œuvres (vidéo, photo, logiciel, etc..).

La réaction de l'employeur

Au sein d'une entreprise, même si le salarié est responsable des sites sur lesquels il navigue et de l'usage qu'il fait de ses outils de communication, il appartient au chef d'entreprise de répondre des actes de ses employés devant les organismes extérieurs.

Par exemple, si le salarié d'une entreprise télécharge des fichiers protégés sans autorisation, l'IP détectée sera celle de l'entreprise, à charge après pour le chef d'entreprise de se retourner contre le salarié fautif.

Outre le fait de télécharger des fichiers, le P2P présente en danger en termes de sécurité, il ne faut pas oublier que ces programmes sont également pourvoyeurs de virus informatiques pouvant potentiellement nuire à la stabilité du réseau de l'entreprise.

Pour prévenir ce risque, il convient d'installer un système de filtre empêchant soit de télécharger le logiciel de P2P, soit de l'installer.

Contrairement à la première menace énoncée, l'entreprise ne peut déduire de la seule présence des fichiers musicaux ou du recours au P2P, une illégalité à tout coup.

Cette illégalité dépend d'une question préalable, ces fichiers ont-ils ou non été téléchargés avec l'accord préalable des auteurs ?

Cette question préalable conduit donc à identifier les contenus afin de déterminer s'il s'agit d'une copie ou d'un original, et donc a vérifié si le salarié a, au préalable obtenu le droit de le télécharger.

Cela étant, une telle analyse nécessiterait trop d'énergie, de temps et des moyens colossaux pour atteindre un objectif de sécurité dont l'efficacité est sérieusement mise en doute puisqu'en définitive, même si elle découvre que l'existence de tels fichiers musicaux, ces derniers auront été téléchargés au moyen d'un équipement de l'entreprise.

En conséquence, les traces que constituent ce téléchargement sur les machines de l'entreprise pourraient donner l'indication aux enquêteurs en ligne que c'est l'entreprise qui est coupable.

Dans une telle hypothèse, l'entreprise pourrait interdire tout recours au P2P, dans une charte d'usage Internet par exemple mais sans s'assurer que cette mesure sera respectée dans la pratique.

De plus pragmatique, elle peut s'en tenir à mettre en garde ses employés contre de telles pratiques, tenter de contrôler la navigation sur Internet, et, surtout, enregistrer les flux entrants et sortants qui transitent au travers de son système informatique pour répondre à toutes éventuelles questions ou interpellations qui pourraient être adressées à l'entreprise quant à ces téléchargements.

Section 3 - Un employé exporte sans autorisation des informations couvertes par le secret de fabrique

Il n'existe pas de définition légale du secret de fabrique. Néanmoins, la jurisprudence l'a défini comme un « *procédé de fabrication offrant un intérêt pratique ou commercial pour l'entreprise qui le met en œuvre, et tenu caché des concurrents qui ne le connaissent pas avant sa violation* ».

Le droit protège ce secret de fabrique de façon négative, puisqu'il punit pénalement sa divulgation, c'est-à-dire sa communication à un tiers par un directeur, ou salarié d'une entreprise où il est employé.

Les peines maximales, prévues à L. 152-7 du Code du travail, et reproduites à l'article L. 621-1 du Code de la propriété intellectuelle, sont de deux ans d'emprisonnement et 30.000 euros d'amende.

Les moyens mis à la disposition de l'employeur

L'entreprise peut juridiquement se protéger contre un tel pillage, par une politique de protection de ses savoir-faire très affûtée.

Concrètement, il s'agit :

d'insérer dans les contrats de travail les dispositions qui lui garantissent de façon exhaustive les droits au titre des créations, inventions de ses salariés (propriété, confidentialité, exclusivité du temps de la présence en entreprise, éventuellement non concurrence au delà de la présence en entreprise, restitution des travaux en fin de contrat, dédit formation, une bonne gestion des outils nomades [ordinateur portable, téléphones mobiles] etc. ...),

- d'insérer aux contrats commerciaux passés avec les partenaires et clients, des clauses qui protègent le secret,
- de mener une bonne politique d'appropriation de ses travaux,
 - soit par les dépôts obligatoires auprès des institutions publiques chargées de recevoir ces dépôts, en France l'Institut National de la Propriété Industrielle - NPI - pour les marques, brevets, dessins et modèles principalement,
 - soit par le recours à des dépôts probatoires pour les droits d'auteur sur logiciels, bases de données ou autres, par exemple en Europe auprès de l'Agence pour la Protection des Programmes⁵, de la Société Logitas⁶, d'un Huissier, d'un Notaire, dans l'enveloppe Soleau de l'INPI etc.

De se défendre, c'est-à-dire de mettre en place une stratégie réfléchie sur comment réagir en cas de risque de copie ou de pillage, y compris et éventuellement par la voie judiciaire.

Section 4 - un salarié consulte des sites pornographiques de son domicile au moyen de l'ordinateur portable de l'entreprise

Cette dernière menace correspond à la question du nomadisme.

De plus en plus souvent, des outils informatiques (ordinateur portable, pda, téléphone mobile, pour l'essentiel) sont mis à la disposition des salariés par l'entreprise afin de leur permettre de travailler à distance.

Cependant, ces outils se diffusent et leur utilisation, jusque dans la sphère privée du salarié et au temps où il n'est plus en activité pour l'entreprise pose le problème de la frontière entre le travail et la vie privée.

La nécessaire protection de la vie privée des salariés

Dans son 24^{ème} Dans son 24^{ème} rapport d'activité, la Commission Nationale de l'Informatique (CNIL) a rapporté un arrêt de la Cour d'Appel de Versailles du 18 Mars 2003 qui est un exemple remarquable de notre scénario.

En l'occurrence, il s'agissait d'un cadre de l'opérateur mobile SFR licencié pour avoir « *détourné l'accès Internet* » de l'entreprise en ayant visité des sites pornographiques

Le salarié, qui avait sept années d'ancienneté, disposait d'un ordinateur portable mis à disposition par SFR pour son activité professionnelle.

L'entreprise avait constaté que son employé s'était connecté à des sites à caractère pornographique et à des sites de jeux.

La Cour constatait que les connexions reprochées avaient pris place « *depuis le domicile du salarié hors du temps et du lieu de travail, mais durant le temps de sa vie privée familiale* ».

En outre, l'employé entendait démontrer que c'était son fils et non lui qui s'était connecté aux sites litigieux, ce que la Cour d'Appel semblait valider.

En conséquence, les juges considéraient que les griefs qui avaient fondé le licenciement du cadre n'étaient pas fondés que dès lors son licenciement était dépourvu d'une cause réelle et sérieuse.

Après « *sept années de collaboration sans faille dans une entreprise importante* », SFR était condamnée à payer à son salarié 54.000 euros de dommages et intérêts pour licenciement abusif.

Section 5 - Copies illicites de logiciels sur les postes de travail

Le statut du logiciel

Depuis une Directive Communautaire de 1991, les logiciels sont comptés parmi les œuvres susceptibles d'être protégées par le droit d'auteur dans l'Union Européenne.

Toutefois, c'est un régime particulier qui a été mis en place.

Le logiciel est ainsi protégé en son code source ou compilé, et en ses matériels dits de conception préparatoire (les différents dossiers d'analyse).

L'auteur bénéficie ainsi de prérogatives patrimoniales d'exploitation et également de droits moraux, passablement érodés en raison de la spécificité de l'œuvre.

La responsabilité de l'entreprise en cas de contrefaçon de logiciel

Aux termes de l'article L.122-4 du Code de la propriété intellectuelle, « *toute représentation ou reproduction intégrale ou partielle [d'une œuvre de l'esprit donc d'un logiciel] faite sans le consentement de l'auteur (...) est illicite* ».

En installant, même de bonne foi, sur le disque dur de son STAD⁷, des logiciels sans disposer du droit de le faire ou en utilisant ce logiciel sans respecter strictement le contrat de licence, vous vous rendez coupable d'actes de contrefaçon.

Aux termes de l'article L.335-4 du Code de la propriété intellectuelle, les peines maximales prévues par la loi pour sanctionner ces actes sont de trois ans de prison et 300.000 euros d'amende.

En pratique bien évidemment, les Tribunaux n'appliqueront pas de sanctions aussi lourdes au simple utilisateur d'un logiciel sans licence.

Cependant, la loi ne fait pas de différence entre le réseau de logiciels piratés et l'utilisateur étourdi incapable de justifier d'une licence sur le logiciel stocké sur son ordinateur ; tous deux sont des contrefacteurs et passibles du même texte pénal ci-avant énoncé.

En effet, la jurisprudence considère que l'entreprise qui a fourni les moyens techniques et technologiques de la copie est susceptible d'être tenue responsable pénalement.

Toutefois, dans la majorité des cas, c'est la responsabilité juridique de l'employeur qui sera mise en jeu, et ce par application de l'article 1384 alinéa 5 du Code civil qui dispose que « *les maîtres et les commettants⁸ [sont responsables] du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés* ».

Cette disposition signifie que tout fait commis par un employé dans l'exercice de ses fonctions et qui cause un dommage à autrui engage systématiquement la responsabilité civile de son employeur.

L'employeur viendra dans ces conditions répondre civilement des fautes de son préposé d'autant que, d'une part, il sera souvent le propriétaire des machines ayant stocké la contrefaçon, d'autre part, c'est l'entreprise qui sera réputée avoir profité directement de la contrefaçon.

Chapitre 2 : Les menaces venant de l'extérieur

Section 1 – La base de données client pillée par des tiers étrangers à l'entreprise : Président, Rssi et Cadres face à leurs juges

Le statut particulier des données à caractère personnel

L'entreprise disposant d'une base de données client doit être vigilante quant au traitement de telles données, dites à caractère personnel au sens de la loi européenne.

Constitue une donnée à caractère personnel l'information qui permet sous quelque forme que ce soit, directement ou non, l'identification d'une personne physique à laquelle elle s'applique (nom, numéro de sécurité sociale, numéro de téléphone...).

Dès l'instant où un système collecte, traite, stocke, archive ce type d'informations, les dispositions de la loi du 6 août 2004, modifiant la fameuse loi relative à l'informatique, aux fichiers et aux libertés du 6 Janvier 1978, s'appliquent.

Il s'en suit que celui qui a le pouvoir de définir le contenu de ce traitement de données à caractère personnel, sa structure, ses finalités, ses conditions de gestion et de communication des données est appelé le responsable du traitement.

C'est à lui qu'incombe les obligations légales de déclaration, d'information préalable des personnes concernées par ces données, d'accès et de correction voire de suppression de ces données.

L'obligation de prendre toutes les précautions utiles

En vertu de l'article 34 de la loi, « *le responsable du traitement est tenu de prendre **toutes précautions utiles**, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

La protection mise en place pour la base de données regroupant des informations à caractère personnel doit ainsi être suffisamment efficace pour lutter contre toutes les atteintes ; celle du simple internaute qui, surfant sur le site, va tenter d'accéder à ce type de données, jusqu'au hacker qui va essayer de s'introduire frauduleusement dans le système.

En pratique, prendre « toutes précautions utiles », signifie essentiellement agir selon l'état de l'art dans le domaine de la sécurité sur le réseau. Aujourd'hui, cela implique pour l'entreprise et pour protéger ce type de contenus de se doter d'un Firewall, de logiciels anti-virus voire d'outils anti-spams, et de les mettre à jour régulièrement.

A défaut, l'employeur s'expose notamment aux peines prévues à l'article 226-22 du Code pénal, punissant de cinq ans d'emprisonnement et de 300.000 euros d'amende « *le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir* ».

Ce délit étant non intentionnel, l'employeur pourrait être tenu responsable de l'imprudence ou de la négligence ayant permis la divulgation d'une donnée à caractère personnel, même à son insu (dans l'hypothèse d'une imprudence ou d'une négligence, les peines maximales étant ramenées à trois ans d'emprisonnement et 100.000 euros d'amende).

Section 2 - l'entreprise impliquée par des propos diffamatoires sur Internet

Liberté d'expression versus responsabilité : application du droit de la presse

Il existe aujourd'hui de nombreux moyens mis à la disposition des internautes souhaitant s'exprimer sur les sujets de leurs choix sur le réseau : les chats, les forums de discussion, ou encore les blogs, les derniers nés du genre.

La finalité de ces forums et autres zones publiques de libre expression est de faire partager un message, une information, aux internautes.

Par principe, si les salariés peuvent revendiquer comme n'importe quel internaute le droit à la liberté d'expression telle que reconnue notamment par l'article 7 de la Convention Européenne des droits de l'homme, ils ne sauraient toutefois porter atteinte aux intérêts de tiers par des propos diffamatoires ou injurieux, et, indirectement, à son employeur qu'il pourrait engager, ne serait-ce que parce que son identité logique qui l'aura servi à s'exprimer révélera l'identité de son employeur.

Pour toutes ces communications publiques qui s'opèrent avec grande facilité sur le réseau, il est admis que le régime de responsabilité qui s'applique est celui du droit de la presse. En effet, dans bien des cas, on peut assimiler la prise de parole sur Internet à une sorte de courrier des lecteurs publiée dans la presse papier.

Outre la responsabilité potentielle de l'hébergeur et de l'éditeur du contenu litigieux, les opinions et avis émis demeurent sous la responsabilité de leur auteur.

Application au cas spécifique du salarié communiquant sur son entreprise

Le salarié peut librement s'exprimer au sujet de son entreprise, sous réserve de la divulgation d'informations confidentielles et du respect de l'ensemble des clauses de son contrat de travail. Il dispose également d'une obligation de loyauté à laquelle il doit s'astreindre conformément à l'article 1134 alinéa 3 du Code civil.

A ce titre, s'il a un droit de critique à l'encontre de son entreprise, y compris sur des espaces publics, ce droit ne doit pas aboutir, soit au dénigrement de son entreprise ni en une attaque personnelle contre ses dirigeants.

Enfin, la limite consécutive à une injure publique ou à une diffamation publique s'applique au salarié comme à tout internaute s'exprimant en des lieux publics de l'Internet, tels que Chat, Forum, listes de discussion par emails etc.

Enfin, le salarié va disposer des moyens de s'exprimer mis à sa disposition par son employeur : ordinateur connecté au réseau localisable par son adresse IP, adresse email faisant ressortir l'identité de l'entreprise dans l'intitulé de l'email de type `dupont@entreprise.fr`.

A priori, l'entreprise ne sera pas mise en cause pour des propos diffamatoires tenus par son salarié à l'encontre de tiers par la seule mise à disposition d'outils par l'entreprise, sauf à démontrer que ces outils ont été mis à disposition en toute conscience. Pour cette raison, dans ce cas, il est important pour l'entreprise de réglementer l'usage de ces outils, notamment aux travers de la charte d'usage Internet, en rappelant que le salarié ne doit pas prendre des positions publiques susceptibles de l'engager.

Section 3 – Un virus déposé sur le site Web de l'entreprise qui devient une passerelle de propagation

Malgré tous les efforts des autorités publiques et des éditeurs d'antivirus, de nouveaux virus informatiques viennent chaque jour, toujours plus nombreux, toujours plus surnois, toujours plus résistants, polluer nos systèmes informatiques et générer des troubles.

Le virus informatique peut être défini comme un logiciel dont la particularité est qu'il se transmet et se reproduit.

Avec le temps, le virus a muté en ver car il se propage désormais par le biais des réseaux. Il est capable de se mettre en sommeil pendant une durée indéterminée ou changer de forme pour tromper les défenses.

Le cheval de Troie est également un programme informatique malveillant qui, une fois introduit dans le STAD, permet d'en prendre le contrôle.

Face au péril que représentent les virus informatiques, et de façon générale la fraude informatique, le législateur a choisi de protéger la société et son ordre social en dotant le Code Pénal de textes répressifs chargés de punir les auteurs de virus dans certains de leurs comportements.

Aux termes de l'article 323-2 du Code pénal, issu de la loi Godfrain relative à la fraude informatique, « *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 75.000 euros d'amende* ».

Fausser le fonctionnement du STAD, c'est lui faire produire un résultat autre que celui attendu par le maître du système : le résultat peut ne pas d'ailleurs être forcément négatif : pour autant le délit est constitué.

Entraver le fonctionnement du STAD signifie le bloquer, totalement ou partiellement, empêcher ou gêner son utilisation ainsi que l'utilisation des applications qu'il stocke.

Mais dans de nombreuses hypothèses, le virus n'est pas qu'un petit programme malicieux, mais un outil puissant de destruction de fichiers ou d'altération de données.

Dans ce cas, on fera application d'un autre article du code pénal, l'article 323-3 qui dispose :

« 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 75.000 euros d'amende ».

Responsabilité potentielle de l'entreprise en cas de transmission du virus par un salarié.

La loi pour la confiance dans l'économie numérique de juin 2004 a créé un nouveau délit à l'article 323-3-1 du Code Pénal.

Ce nouvel article dispose que :

« Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ».

A priori, le salarié qui, de bonne foi se voit infecter par un virus qui pourrait lui être transmis par courrier électronique puis le retransmet par un même moyen à un nouveau destinataire, ne devrait pas être inquiété dans la mesure où l'intention coupable nécessaire à la commission de toute infraction pénale ferait défaut (article L. 121-3 du Code pénal).

L'entreprise doit mettre au point un arsenal tant juridique que technique, en vue de palier les attaques de plus en plus perfectionnées et nombreuses.

En cas de contentieux, il appartiendra au juge d'évaluer les précautions prises par l'entreprise, afin d'apprécier l'existence ou non de sa responsabilité. Si celle-ci a pris un certains nombres de diligences, eu égard à l'état de l'art dans le domaine, elle ne craindra pas de voir sa responsabilité engagée. Il en va de même pour l'entreprise qui est contaminée par « la première vague de virus » dont on ne connaît pas encore le moyen d'y remédier.

En revanche, sa responsabilité pourrait être retenue dans l'hypothèse où le virus qui s'est propagé est apparu depuis plusieurs mois et que l'employeur n'a pas mis en place des systèmes de sécurité suffisamment efficaces. En effet, cette omission est susceptible de constituer une faute civile au sens de l'article 1383 du Code civil, disposant que « *chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence* ». Si la faute revient à l'un de ses salariés, la responsabilité civile de l'employeur pourrait être engagée sur le fondement de l'article 1384 alinéa 5, au titre de la responsabilité de l'employeur pour les fautes commises par le salarié dans l'exercice de ses fonctions, la jurisprudence ayant adopté une définition très large de « l'exercice des fonctions ».

Section 4 - L'identité de l'entreprise usurpée

L'usurpation d'identité sanctionnée sous condition

L'usurpation d'identité se retrouve de plus en plus couramment sur Internet et dans des situations très diverses.

Derrière ce délit peut se cacher une volonté de spammer, de tenter une escroquerie à la carte bancaire ou encore de diffamer.

L'expression la plus récente de cette usurpation d'identité est ce que l'on nomme le « phishing ». Il s'agit le plus souvent d'un phénomène conduisant les internautes à communiquer leurs coordonnées bancaires suite à l'envoi d'un mail au nom d'un établissement bancaire.

L'usurpation d'identité n'est pas un délit pénal en tant que tel, elle le devient dès l'instant où « *le fait de prendre le nom d'un tiers, [a été opéré] dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales* » (article 434-23 du Code Pénal). Elle est alors punie de cinq ans d'emprisonnement et de 75.000 euros d'amende.

La condition, pour que le délit soit constitué, tient à ce que ait été pris « le nom d'un tiers ». Néanmoins il n'existe pas de jurisprudence affirmant que « prendre » une adresse IP ou une adresse email est assimilable au « nom » de l'article 434-23 précité.

Le délit pourra prendre la forme d'une escroquerie en cas de motivation financière, puisqu'il s'agira de tromper une personne par l'usage d'un faux nom ou d'une fausse qualité. Le délit de faux pourra également être retenu dans certaines hypothèses.

Sur le plan civil, il est possible de réprimer l'usurpation d'identité par le biais de l'article 1382 du Code civil, exigeant la démonstration d'une faute, d'un préjudice subi par la victime et d'un lien de causalité entre les deux.

Par exemple, la révélation par l'usurpateur de l'intimité de l'usurpé est susceptible d'être condamné par le recours à l'application combinée des articles 9 relatif à la protection de la vie privée, et 1382 du Code civil.

Egalement, si le nom patronymique de la victime a été reproduit dans un nom de domaine, là encore, ce cas dit de cybersquatting pourra être sanctionné civilement.

Les recours à la technique pour l'authentification et contre l'usurpation d'identité

Par les techniques d'authentification, il s'agit de sélectionner à l'entrée d'un système les candidats qui se présentent à l'effet de ne laisser pénétrer que ceux disposant de droits d'accès.

Bien évidemment, la finalité d'une telle authentification consiste à interdire l'accès au système à un intrus sans droits quel que soit son mobile, pénétration dans un but de vol d'informations, de sabotage ou même de simple visite. L'authentification d'un utilisateur à l'entrée du système se fait habituellement selon au moins l'un des trois critères suivants :

- Critère 1 : ce que sait l'utilisateur,
- Critère 2 : ce que possède l'utilisateur,
- Critère 3 : ce qu'est l'utilisateur.

- **En ce qui concerne le premier critère**, « ce que sait le candidat à l'accès », c'est le plus souvent un identifiant (login) et un mot de passe (Password) géré par un système autonome.

Ce code lui a été confié par le maître du système. Si on se trouve dans une relation de travail, la notion de garde du code d'accès et de responsabilité à son égard, se trouve souvent incluse dans les chartes d'usage Internet des entreprises.

Le code d'accès et le mot de passe peuvent se trouver à distance, c'est-à-dire résider sur le système lui-même, comme un code d'accès à un immeuble.

- **Selon le second critère**, « ce que possède un candidat », c'est la clef, la carte l'autorisant à pénétrer dans le système.

- Enfin, **selon le troisième critère**, « ce qu'est l'utilisateur », c'est le recours à la technologie biométrique qui se définit habituellement comme la science des variations biologiques.

Elle comporte deux grandes applications : l'identification d'une personne au sein d'un groupe de personnes et l'authentification d'une personne se présentant à l'entrée d'un système d'information, voire d'un local physique.

Seule cette seconde application nous intéresse ici, s'agissant des systèmes d'information. Cette technologie fait appel aux caractéristiques physiques de ceux qui détiennent un droit d'accès, on parle alors de reconnaissance biométrique.

Le principe est simple : chacun est son propre authentificateur. De l'empreinte digitale, au contour de la main, à l'empreinte vocale en passant par l'empreinte rétinienne, toutes les reconnaissances physiques sont en théorie légalement admissibles. On dit que la biométrie est la forme la plus ancienne d'authentification.

Les animaux eux mêmes l'utiliseraient à leur façon.

On parle d'authentification forte lorsque deux des trois critères précités se combinent pour authentifier. Par exemple, les code et mot de passe se trouvent détenus par le porteur lui-même, comme le code confidentiel d'une carte bancaire enregistré sur la puce de la carte elle-même et gérant l'accès aux terminaux de paiement.

Pour revenir à la biométrie, les experts techniques voient au passif de cette technologie, d'une part, son coût, d'autre part, la question de sa révocation. En effet, face à une personne qui a subtilisé un mot de passe ou une signature électronique, le titulaire du mot de passe ou de la signature peut le remplacer ou le révoquer.

En revanche, comment faire s'il y a « vol » de l'empreinte digitale ou rétinienne ? Si un tiers s'approprie une telle identité biométrique, il peut passer tout type d'actes au nom du titulaire de l'identité usurpée. Si les experts en sécurité prétendent disposer de solutions à ce problème, ils y reconnaissent cependant là une difficulté au passif de cette protection technique. Or, pour le juriste, une telle difficulté ne peut être envisagée que sous l'angle technique, elle doit également être vue sous l'aspect social. C'est la raison principale du traitement d'exception réservé à la biométrie dans l'arsenal législatif français et européen. Bien qu'autorisée, la biométrie n'en est pas moins sous surveillance, car jugée dangereuse pour le citoyen.

Section 5 - L'attaque rebond et poste zombie

Tout ordinateur connecté à un réseau informatique est potentiellement susceptible de se faire attaquer. Sur Internet, des attaques ont lieu en permanence, lancées automatiquement à partir de machines infectées généralement à l'insu de leur propriétaire, ou directement par un pirate informatique.

L'attaque par rebond est une technique sophistiquée consistant à s'attaquer tout d'abord à une cible intermédiaire, donc une première machine, afin de masquer l'adresse IP réelle du pirate et d'utiliser les ressources de cette machine servant de rebond.

Ensuite, le cyberdélinquant peut rebondir et mener à partir de cette machine piratée son attaque sur une cible finale. La première machine se retrouve ainsi complice contre son gré de l'attaque.

Il s'agit en quelque sorte d'une usurpation d'identité du STAD piraté à l'insu de son maître qui va se retrouver le premier interrogé en cas de litige.

Les propriétaires des machines piratées sont donc victimes d'un accès frauduleux à leur système, tel que décrit à l'article 323-1 du Code pénal, et puni de deux ans d'emprisonnement et 30.000 euros d'amende à 3 ans d'emprisonnement et 45.000 euros d'amende selon les hypothèses.

Les preuves constituées par les maîtres des machines piratées

Il existe une liberté totale de preuve dans la mesure où le rebond, ainsi que l'acte d'accéder frauduleusement à un STAD sont des faits juridiques. Aussi, la personne victime d'un rebond pourra parfaitement prouver son innocence dans l'attaque finale par la production en justice de tout élément de preuve, y compris une donnée technique de connexion ou un log de connexion.

En outre, depuis la loi du 13 mars 2000, la notion de preuve littérale ou par écrit est désormais admise quelque soit le support, même électronique.

Ainsi, le nouvel article 1316 du Code Civil issu de la loi dispose que :

« La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tout autre signe ou symbole doté d'une signification intelligible, quels que soient leurs supports et leurs modalités de transmission. »

Quant à l'article 1316-1, il précise que :

« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. »

L'écrit peut donc désormais également résulter de « tout signe ou symbole ... » quel qu'en soit le support, à condition qu'il soit doté d'une signification intelligible.

Ces deux premiers points de la réforme fondent le principe dit de **neutralité technique et de non discrimination** à l'égard d'un média ou d'un support. Pour la première fois, l'écrit n'est plus assimilé à un support, il en est totalement indépendant.

En conséquence, les données techniques de connexion sont des preuves admissibles ou en tout état de cause qui ne pourront être d'emblée rejetées par un juge.

Un problème peut néanmoins subsister : L'attaque rebond pourra se révéler au maître du système intermédiaire, plusieurs jours, semaines ou mois après qu'elle ait été réalisée.

Celui-ci devra conserver les données prouvant son innocence d'une part, et des éléments d'identification sur l'attaquant d'autre part, afin de pouvoir les présenter dans des délais très brefs si besoin est.

Il s'agit donc de produire les données de connexion enregistrées sur le STAD intermédiaire qui vont venir démontrer l'attaque puis le rebond jusqu'au STAD final.

Conclusion

« Victime et peut être responsable », voilà le nouvel axiome auquel les entreprises sont susceptibles de faire face.

Dès lors, une politique de sécurité s'impose, par l'organisation, la technique et la pédagogie.

C'est une nouvelle culture de nouveaux gestes au moyen de nouveaux outils que l'entreprise doit acquérir.

Ces premiers gestes sont destinés à la protéger et à dégager sa responsabilité juridique.

Désormais, le concept de la « Compliance » doit servir de guide pour mettre en place une nouvelle organisation de la Société et doit orchestrer l'ensemble de sa gestion interne afin de s'assurer la mise en conformité de l'entreprise avec la réglementation, les normes et l'éthique de l'entreprise.

Pour atteindre cet objectif de conformité aux lois et autres règles normatives, une entreprise doit : déterminer précisément les risques potentiels en identifiant le corps de réglementation à que cette dernière doit respecter
organiser la gestion des risques auxquels l'entreprise doit faire face dans ses activités de tous les jours.

Concrètement, appliquer à la sécurité informatique, la « Compliance » peut être résumé en un ensemble de règles que les entreprises doivent respecter et qui est résumé ci-après :

1. Le respect de la boîte à lettre électronique du salarié

2. L'usage raisonnable des biens de l'entreprise par les salariés

3. La rédaction d'une charte d'usage de l'internet implique le respect de trois principes :

- une information préalable des salariés
- le recueil de l'avis des organes représentatifs du personnel
- un contrôle mesure et proportionnel à l'objectif poursuivi

4. La traçabilité des flux d'informations transitant via les postes informatiques de l'entreprise ne doit pas se faire au mépris du respect de la vie privée des salariés

5. La protection des données à caractère personnel

6. L'organisation d'audits et de contrôles internes, conformément à la Loi Sarbanes-Oxley et l'Accord Bâle II

7. La désignation d'un responsable pour appliquer l'ensemble de ces règles

Contacts Régionaux:

Websense France

Paris
tel +33 (0) 1 56 60 58 14
fax +33 (0) 1 56 60 56 00
www.websense.com/fr

Websense, Inc.

San Diego, CA USA
tel +1 800 723 1166
fax +1 858 458 2950
www.websense.com

Websense UK Ltd.

Reading, Berkshire UK
tel +44 118 938 8600
fax +44 118 938 8698
www.websense.co.uk

Websense Ireland

Dublin Ireland
tel +353 1 6319360
fax +353 1 6319001
www.websense.com

Autres adresses

www.websense.com/international

Sites Nationaux:

Australie websense.com.au	Israël websense.com
Chine prc.websense.com	Italie websense.it
France websense.fr	Japon websense.jp
Allemagne websense.de	Pays-Bas websense.com
Hong Kong websense.cn	Singapour websense.com
Inde websense.com	Espagne websense.com.es
Irlande websense.co.uk	Emirats Arabes Unis websense.com

Téléchargez une version gratuite utilisable 30 jours sur
www.websense.com/downloads