

Ouverture des systèmes vs sécurité



10 scénarios pour comprendre et répondre
aux nouveaux risques juridiques

Sommaire

Le mot d'accueil de Websense	1	Le statut particulier des données à caractère personnel	6	Scénario 8	
Interview	2	L'obligation de prendre toutes les précautions utiles	6	Un salarié consulte des sites pornographiques de son domicile au moyen de l'ordinateur portable de l'entreprise	10
Scénario 1		Scénario 5		La nécessaire protection de la vie privée des salariés	10
« des fichiers pédophiles sur le serveur de l'entreprise (proxy de navigation sur le web) »	3	l'entreprise impliquée par des propos diffamatoires sur Internet	7	Scénario 9	
Contenus pédophiles = contenus illégaux	3	Liberté d'expression versus responsabilité : application du droit de la presse	7	Copies illicites de logiciels sur les postes de travail	11
Les gestes pour dénoncer et dégager sa responsabilité	3	Application au cas spécifique du salarié communiquant sur son entreprise	7	Le statut du logiciel	11
Scénario 2		Scénario 6		La responsabilité de l'entreprise en cas de contrefaçon de logiciel	11
Un salarié télécharge sur le lieu de travail des fichiers musicaux pirates en P2P	4	Un virus déposé sur le site Web de l'entreprise qui devient une passerelle de propagation	8	Scénario 10	
Le P2P, une pratique légale qui devient illégale sous conditions	4	Les virus informatiques, sanctionnés par la Loi Godfrain	8	l'attaque rebond et poste zombie	12
La réaction de l'employeur	4	Responsabilité potentielle de l'entreprise en cas de transmission du virus par un salarié	8	Les sanctions de l'attaque par rebond	12
Scénario 3		Scénario 7		Les preuves constituées par les maîtres des machines piratées	12
Un employé exporte sans autorisation des informations couvertes par le secret de fabrique	5	L'identité usurpée	9	Conclusions	12
Le secret de fabrique, protégé par la Loi	5	L'usurpation d'identité sanctionnée sous condition	9		
Les moyens mis à la disposition de l'employeur	5	Les recours à la technique pour l'authentification et contre l'usurpation d'identité	9		
Scénario 4					
La base de données client pillée par des tiers étrangers à l'entreprise : Président, Rssi et Cadres face à leurs juges	6				

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 :

- 99% des entreprises utilisent un logiciel anti-virus, 78% d'entre elles ont été attaquées par des virus, vers, etc. (CSI/FBI Computer Crime and Security, 2004) [Rapport sur la sécurité et la délinquance informatique]
- Une étude portant sur trois millions d'ordinateurs professionnels a recensé 83 millions d'instances de logiciels espions. (Groupe Gartner, septembre 2004)
- « Les pertes mondiales inhérentes aux cyber-attaques représentaient environ 16,7 milliards de dollars fin 2004, contre 3,3 milliards de dollars en 1997. » (Computer Economics, 2004)

La solution Websense

Websense® Web Security Suite™ fournit une solution de sécurité Web intégrée qui comble les écarts technologiques et temporels laissés ouverts par les solutions de sécurité existantes.

Websense Web Security Suite bloque les logiciels espions, les codes malveillants (MMC) et autres menaces en ligne, ainsi que les transmissions des logiciels espions et des keyloggers vers leurs sites hôtes. Elle protège également les employés du phishing et contrôle l'envoi et la réception de pièces jointes à travers les clients de messagerie instantanée (MI). Websense Web Security Suite fournit des mises à jour en temps réel pour une protection immédiate contre les nouvelles menaces de sécurité et inclut des outils de création de rapports et d'analyse performants qui fournissent aux entreprises des informations complètes sur l'accès des utilisateurs à des sites frauduleux ou sur leur vulnérabilité relative aux codes malveillants.

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 ; Il a été rédigé par Maître Olivier ITEANU, Avocat auprès de la Cour d'Appel de Paris, membre de l'Internet Corporation for Assigned Names and Numbers (ICANN) dont il a été membre d'une commission statutaire, auteur de nombreux ouvrages qui traitent du droit des technologies de l'information depuis le début de l'Internet.

Elle lui a demandé de restituer une information honnête, fidèle et surtout accessible aux non juristes, d'où la présentation de ce livre blanc par scénarios avec des analyses et des réponses sous forme de fiches facilement accessibles.

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 !

Philippe BIROT
Directeur Europe du Sud
Websense

Interview

Websense : On voit fleurir dans les entreprises européennes une pratique consistant à rédiger des chartes d'usage Internet pour les membres de l'organisation : la signature de telles chartes par les employés déresponsabilise-t-elle l'entreprise et ses dirigeants au titre des flux entrant et sortant qui transitent par le système d'information de l'entreprise ?

Olivier Iteanu : Honnêtement, non. A l'origine, les chartes d'usage Internet étaient avant tout un document pédagogique sans valeur juridique. Il s'agissait d'élever le niveau de culture de la communauté des personnes vivant et travaillant au sein de l'entreprise par rapport à l'usage des nouveaux outils de communication et les risques susceptibles de faire courir à l'entreprise. 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 rejoindre un « tiroir » préexistant dans la liste des normes juridiques nombreuses qui existent dans le monde du travail : il s'agit soit du règlement intérieur de l'entreprise qui est une norme juridique contraignante unilatéralement écrite par l'employeur et qui est très étroite de ce fait car le législateur se méfie de tout ce qui ne vient que de l'employeur, soit du contrat de travail de l'employé qui est une 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. Enfin, la charte peut rejoindre une norme juridique de plus bas niveau, qu'est la simple note de service. Mais ces manipulations comportent deux limites. D'une part, la validité de la charte et son opposabilité au salarié pourra toujours être contestés par la suite. Il y a très peu de jurisprudence à ce jour sur ces questions mais on sait déjà que certains syndicats ont élevé la voix pour dire le mal qu'ils pensaient de certaines chartes qui allaient trop loin dans la responsabilisation des salariés. On peut parier que les Tribunaux annuleront certaines dispositions de

certaines chartes bientôt. D'autre part, et c'est le point le plus important à mes yeux, la charte ne fait qu'éduquer et donner des recours à l'entreprise vis à vis de ses membres en cas de manquement de leur part si elle est reconnue de valeur juridique. Elle ne protège pas a priori l'entreprise contre les cas de fraude ou d'attaque. Pour atteindre ce premier but, il est sur que la technique est ici plus adaptée que le droit qui ne vient qu'après le sinistre.

Websense : Existe-t-il en droit français et même européen, des spécificités relatives à la protection technique des entreprises pour se prémunir contre les cas de fraude ou d'attaque contre leur système d'information ? En d'autres termes, certaines technologies sont-elles a priori illégales

Olivier Iteanu : Non, c'est absurde, ça n'est certainement pas au législateur européen de trier entre telle ou telle technologie, sauf des cas d'utilisation de technologie extrême comme la biométrie, technologie contre laquelle se dessine actuellement en France et en Europe des règles de droit de défiance. En dehors de ces cas très particuliers, on peut affirmer qu'il n'existe aucune règle juridique française ou européenne qui vienne dicter aux entreprises le recours à tels outils techniques plutôt que tels autres. De ce point de vue, les entreprises françaises et européennes peuvent recourir à tout type de techniques pour, par exemple, filtrer des contenus juridiquement illégaux, c'est-à-dire portant atteinte soit à l'ordre public, comme la pédophilie, les contenus racistes, négationnistes, ou portant atteinte aux droits des tiers, comme les contenus diffamants, injurieux ou contrefaisant vis-à-vis de la musique de vidéo, des jeux ou autres. Ici, le meilleur conseil à donner à l'entreprise est de recourir à la meilleure technologie qui dispose de la plus grande expérience et du meilleur savoir-faire. C'est une attitude universelle et aucun législateur au monde ne viendra la contredire, compte tenu des enjeux primordiaux que représente une bonne protection technique pour les entreprises du pays.

Websense : Une entreprise peut-elle être attaquée en justice par l'un de ses employés pour « détention d'information personnelle et potentiellement discriminatoire à son égard » en cas de contrôle des allers et venus sur le système d'information de l'entreprise ?

Olivier Iteanu : Il existe bien sur des conditions de légalité préalable à respecter, principalement au regard de la législation du travail (information préalable des salariés par voie d'affichage ou de note de service sur la mise en place d'un contrôle, avis préalable des représentants du personnel, respect d'un principe dit de proportionnalité, c'est-à-dire justifier le recours au contrôle par les risques juridiques liés à l'ouverture du système) et au regard des lois européennes relative à l'informatique et aux libertés. En France, cela signifiera essentiellement déclarer l'existence d'un traitement qui consiste à collecter les traces d'entrée et de sortie au travers du système auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL). Ces formalités légales préalables doivent bien évidemment être respectées. Elles sont tout à fait logiques parce qu'il est juste que des gardes fous soient posés à la cybersurveillance, mais au final constituent des contraintes assez légères pour l'entreprise. En dehors de cela, il n'y a aucune illégalité ou discrimination qui pourrait être reprochée par principe à une entreprise qui met en place ces contrôles pour se protéger, droit qui lui est tout à fait reconnu.

Scénario 1 « Des fichiers pédophiles sur le serveur de l'entreprise (proxy de navigation sur le web) »



Contenus pédophiles = contenus illégaux

Les deux principaux services de l'Internet, le Web et l'email, ont donné accès à des contenus en grande quantité et de qualité inégale.

Cette débauche d'échanges et de contenus ne concerne pas toujours des contenus licites. De manière très minoritaire, les contenus pédophiles s'affichent et se diffusent aussi sur le Net.

S'agissant de la pédophilie, les experts considèrent que cette déviance a trouvé avec Internet un terrain propice à un certain développement.

Dans l'ensemble de l'Europe, la simple visite d'un site pédophile est sanctionnée : 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 »

Les sanctions sont lourdes, soit 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. »

« 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. »

On passe, enfin, à dix ans de prison et 500.000 euros d'amende, comme peine maximale, lorsque ce délit est commis en bande organisée.

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 commettants [sont responsables] du dommage causé par leurs domestiques et préposés 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 1998, 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.

Scénario 2 – Un salarié télécharge sur le lieu de travail des fichiers musicaux pirates en P2P

Le P2P, une pratique légale qui devient illégale sous conditions

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'échanges.

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

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

A la différence du scénario 1, l'entreprise ne peut déduire de la seule présence des fichiers musicaux ou du recours au P2P, une illégalité à tout coup.

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. »

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

La question préalable impose donc une sorte d'audit des contenus : quels sont-ils ? A-t-on obtenu le droit préalable de le télécharger : en clair est-ce une copie ou un original ?

Cela étant, l'entreprise ne peut effectuer une telle analyse. Elle dépenserait trop d'énergie, de temps et des moyens colossaux pour atteindre un objectif de sécurité au final tout de même aléatoire, car même si elle découvre après coup des fichiers musicaux, il n'empêche que le fichier sera bien là téléchargé sur les machines de l'entreprise au moyen d'un équipement de l'entreprise. Tout cela laisse des traces qui pourraient donner l'indication aux enquêteurs en ligne que c'est l'entreprise qui est coupable.

Que peut faire dès lors l'entreprise dans un tel cas ?

Interdire tout recours au P2P, dans une charte d'usage Internet par exemple ?

Elle peut le faire et l'écrire, sans garantie que cela sera suivi dans la pratique.

Elle peut aussi, ce qui nous paraît plus pragmatique, s'en tenir à mettre en garde ses employés contre de telles pratiques, tenter de contrôler la navigation sur Internet, et, surtout, enregistrer les va et vient au travers de son système pour répondre demain à toutes questions ou interpellations qui pourraient lui être adressées sur ce thème.

Scénario 3 – Un employé exporte sans autorisation des informations couvertes par le secret de fabrique



Le secret de fabrique, protégé par la Loi

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 connaissaient 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, en premier lieu par une politique de protection de ses savoir-faire très affûtée.

Il s'agit

- d'insérer aux contrats de travail les dispositions adéquates qui lui garantissent 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 – INPI - pour les marques, brevets, dessins et modèles principalement, soit par le recours à des dépôts dits 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 Programmes, de la Société Logitas, 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.

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.

Scénario 4 – 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.

Au sens de la loi européenne, ces données sont des données dites à caractère personnel.

Une donnée à caractère personnel est une 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, le régime de ces données tombe dans celui des données à caractère personnel jusqu’à ce jour régi par les dispositions de la fameuse loi relative à l’informatique, aux fichiers et aux libertés du 6 Janvier 1978, récemment modifiée par la loi du 6 août 2004.

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 déclaratives, d’information préalable, d’accès et de correction voire suppression à celui concerné par des données, de conservation des 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

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 ».

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 personnelles doit ainsi être suffisamment efficace pour lutter contre toutes les atteintes ; celle du simple internaute qui, surfant sur le site, ne doit pas pouvoir accéder à ce type de données, jusqu’au hacker qui va tenter 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).

Scénario 5 – 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 autre 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 reconnu 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.

L’entreprise peut elle être responsable pour des propos diffamatoires tenus par son salarié à l’encontre de tiers, aux moyens des outils mis à la disposition par l’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 priori, l’entreprise ne sera pas mise en cause par la seule mise à disposition d’outils, 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.

Scénario 6 – Un virus déposé sur le site Web de l’entreprise qui devient une passerelle de propagation

Les virus informatiques, sanctionnés par la Loi Godfrain

Malgré tous les efforts des autorités publiques et des éditeurs d’antivirus, de nouveaux virus informatiques viennent chaque jour, toujours plus nombreux, toujours plus sournois, 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 ».

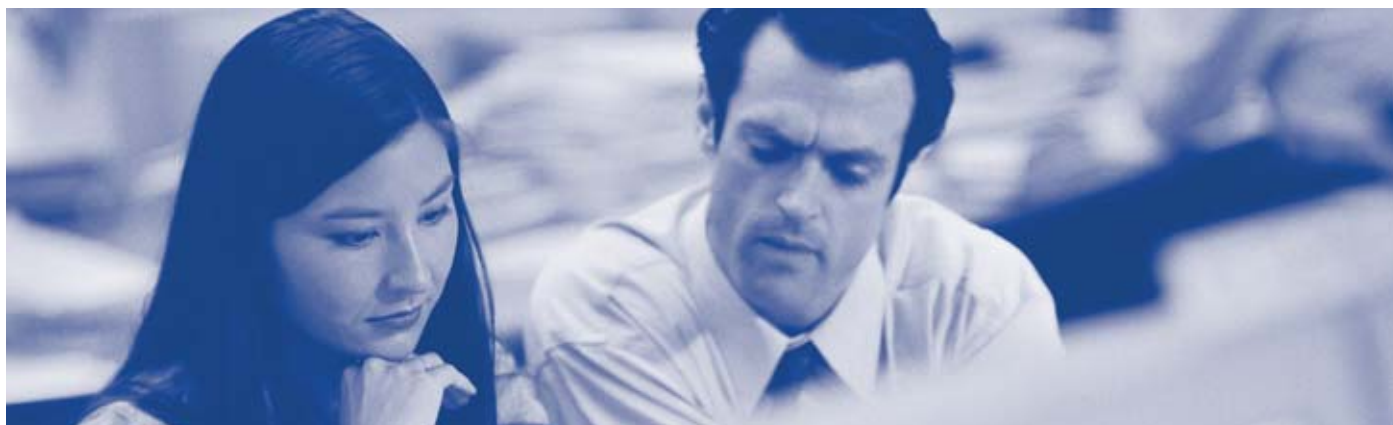
A priori, le salarié qui, de bonne foi se voit infecter par un virus qui pourrait lui être transmis par courrier électronique puis le retransmet par un même moyen à un nouveau destinataire, ne devrait pas être inquiété dans la mesure où l’intention coupable nécessaire à la commission de toute

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 certain nombre 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 » (cf. scénario 1).



Scénario 7 – L’identité 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.

Ce que sait le candidat à l’accès, c’est le plus souvent un identifiant (login) et un mot de passe (Pin Code) 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 critère n°3, 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 sociétal. 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.

Scénario 8 - Un salarié consulte des sites pornographiques de son domicile au moyen de l'ordinateur portable de l'entreprise



C'est ici le problème du nomadisme.

De plus en plus, les salariés des entreprises disposent d'outils mis à disposition de l'entreprise qui leur permettent de travailler à distance de là où ils se trouvent : c'est l'ordinateur portable, le simple pda, le téléphone mobile pour l'essentiel.

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 24ème 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.

Scénario 9 – 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 STAD, 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.

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 ».

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 commettants [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.

Scénario 10 – L’attaque rebond et poste zombie

Les sanctions de l’attaque par rebond

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 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 (appelé Système de Traitement Automatisé de Données ou STAD dans la Loi française), 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.

Conclusions

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

Ils peuvent être résumés comme suit, à partir de la connaissance d’une attaque, d’un sinistre :

Rechercher les éléments de preuve techniques pour connaître la vérité des faits : par exemple, comment tel fichier a été introduit sur le serveur

Déterminer l’identité logique (url) de la machine par qui le problème se pose

Rechercher éventuellement dans les fichiers de log de connexion pour déterminer l’adresse IP interne de la machine à problème

Prendre ensuite les mesures juridiques de sauvegarde qui s’imposent, comme recourir à un Huissier de Justice pour faire dresser un procès-verbal qui fige la réalité technique assisté ou d’un expert indépendant de l’entreprise.

Mener seulement ensuite les actions juridiques appropriées, comme porter plainte par lettre recommandée AR auprès du Procureur de la République près le Tribunal de Grande Instance dans le ressort duquel est situé l’entreprise, joindre les preuves collectées et mises en forme selon une forme familière au système judiciaire.

En plus ...

Mettre en place une cybersurveillance légale

Mettre en place une charte d’usage Internet

A propos de Websense

Websense, Inc. (Code NASDAQ : WBSN) est le premier éditeur mondial de la sécurité des accès Internet. Websense permet aux entreprises d'optimiser l'utilisation des ressources informatiques par leurs employés et de réduire les nouvelles menaces liées à l'utilisation d'Internet, comme la messagerie instantanée, le peer-to-peer, les logiciels espions. En fournissant des produits capables de faire appliquer et respecter les politiques d'utilisation d'Internet au niveau de la passerelle, du réseau et du poste de travail, Websense améliore la productivité et la sécurité, optimise l'utilisation des ressources informatiques et réduit la responsabilité légale pour ses clients. Websense compte plus de 24 000 clients à travers le monde, ce qui représente plus de 20 millions de postes.

Pour toute information complémentaire, rendez-vous sur le site www.websense.com.



Websense, France SARL
54/56 Avenue Hoche
75008 Paris
France
Tel: +33 (0) 156 60 5814
www.websense.fr